Citrix® MetaFrame XP™ Server
for Windows®
With Feature Release 3

Citrix Systems, Inc.
Contents

Chapter 1  Welcome

MetaFrame XP Documentation .................................................. 14
Using PDF Documentation ......................................................... 15
Documentation Conventions ....................................................... 15
Using Online Help ................................................................. 16
Providing Feedback about this Guide ........................................... 16
Finding Information about Windows Servers ................................. 16
Citrix on the World Wide Web .................................................. 17

Chapter 2  Introduction to MetaFrame XP Server

Overview of Server-Based Computing ......................................... 19
Components of Server-Based Computing ...................................... 20
Overview of MetaFrame XP Server Farms ..................................... 20
Independent Management Architecture (IMA) .............................. 21
Independent Computing Architecture and ICA Clients .................... 22
Citrix ICA Clients ................................................................. 22
Overview of the MetaFrame XP Family ........................................ 23
Features of MetaFrame XP for Windows ....................................... 23
  Application Server Features ..................................................... 23
  Citrix ICA Client Features ..................................................... 24
MetaFrame XP Feature Releases ................................................ 26
  Features Included in Feature Release 3 ..................................... 26
  Features Included in Feature Release 2 ..................................... 33
  Features Included in Feature Release 1 ..................................... 37
  Features in MetaFrame XP ..................................................... 40

Chapter 3  Planning for MetaFrame XP Deployment

System Requirements ............................................................... 43
System Software Requirements .................................................. 43
System Hardware Requirements .................................................. 45
Sizing Systems for MetaFrame XP ............................................. 47
## Chapter 4 Installing MetaFrame XP

Creating the Data Store with SQL Server, Oracle, or DB2 .................................. 105
Changing Server Drive Letters .................................................................................. 107
Using the MetaFrame XP Windows Installer Package ............................................. 108
  Common Windows Installer Commands ............................................................... 108
  Creating a Log File ............................................................................................... 109
Unattended Setup of MetaFrame XP Servers ............................................................. 110
  Applying Transforms ......................................................................................... 110
  Creating an Answer File ..................................................................................... 111
Starting MetaFrame XP Setup .................................................................................... 112
Choosing Options During Setup .............................................................................. 113
  Selecting the MetaFrame XP Family Level .......................................................... 113
  Choosing the Product Type .................................................................................. 114
  Selecting Components ....................................................................................... 114
  Creating a New MetaFrame XP Server Farm ....................................................... 115
Joining an Existing MetaFrame XP Server Farm ......................................................... 116
Configuring the Data Store ...................................................................................... 116
  Assigning Farm Administrator Credentials ....................................................... 123
Configuring Session Shadowing .............................................................................. 123
Configuring Network ICA Connections .................................................................. 125
Installing the Web Interface for MetaFrame XP ...................................................... 125
  Configuring the Citrix XML Service Port ............................................................ 125
  Setting the Server’s Default Web Page ............................................................... 127
Installing ICA Client Software ................................................................................. 127
Upgrading to MetaFrame XP Feature Releases ....................................................... 129
Downgrading to a Previous MetaFrame XP Feature Release ................................. 130
Setting a Server’s Feature Release Level .................................................................. 130
Migrating to MetaFrame XP ..................................................................................... 131
  Supported Migration Paths .................................................................................. 131
Cloning a MetaFrame XP Server ............................................................................. 133
Uninstalling MetaFrame XP ..................................................................................... 133
Installing the Management Console for MetaFrame XP on Other Computers ....... 134
  Updating the Management Console for MetaFrame XP ...................................... 135
## Chapter 5  Licensing MetaFrame XP

Overview of MetaFrame XP Licensing ..................................... 137  
Summary of the Licensing Process ......................................... 138  
Types of MetaFrame XP Licenses ........................................... 140  
  Product Licenses .............................................................. 140  
  Connection Licenses .......................................................... 141  
  Migrating Licenses from Earlier Versions of MetaFrame .......... 141  
  Upgrading Licenses ............................................................ 142  
Understanding MetaFrame XP Licensing Codes ....................... 142  
  Product Codes ................................................................. 143  
  Serial Numbers ............................................................... 144  
  License Numbers ............................................................. 146  
  License Activation Codes .................................................. 146  
Managing and Monitoring Licenses ......................................... 147  
  Adding Licenses to Server Farms ......................................... 148  
  Activating Licenses ........................................................... 148  
  License Views ................................................................. 149  
Managing License Counts .................................................... 152  
  Pooling License Counts .................................................... 153  
  Assigning License Counts ................................................ 153  
  Removing Licenses ........................................................... 154  
  Client Device Licensing .................................................... 154  
Licensing Requirements for MetaFrame XP Feature Releases ........ 154  
  Activating Feature Release Licenses .................................... 154  
  Viewing Feature Release License Information ......................... 156

## Chapter 6  Securing MetaFrame XP Deployments

Overview of Securing MetaFrame XP Deployments ..................... 159  
Overview - Deploying SSL Relay ........................................... 161  
Overview - Deploying the Secure Gateway for MetaFrame ......... 161  
Overview - Deploying ICA Encryption .................................... 162  
Setting up Citrix SSL Relay .................................................. 162  
  Deploying MetaFrame with SSL Relay ................................ 162  
  Upgrading SSL Relay from Feature Release 1 ......................... 168
## Chapter 7 Configuring MetaFrame XP Servers and Farms

Management Tools for MetaFrame XP ........................................ 169  
Overview of MetaFrame XP Management Tools .......................... 170  
The ICA Administrator Toolbar ............................................. 171  
The Management Console for MetaFrame XP ............................ 173  
Configuring MetaFrame XP Administrator Accounts .................. 174  
Using the Management Console for MetaFrame XP ..................... 177  
Data Displayed in the Management Console ............................. 178  
Citrix Web Console ............................................................ 181  
Configuring MetaFrame XP Properties ...................................... 182  
Properties of MetaFrame XP Server Farms ............................... 182  
Using the Farm Properties Page .......................................... 182  
Configuring MetaFrame XP Server Properties ............................ 186  
Using the Server Properties Page ....................................... 186  
Configuring Zones and Data Collectors ................................. 189  
Functions of Data Collectors ............................................. 190  
Configuring Latency Reduction for ICA Clients ......................... 192  
Deploying SpeedScreen Settings ......................................... 193  
Improving Responsiveness with SpeedScreen Browser Acceleration ... 193

## Chapter 8 Configuring ICA Connections

Overview of ICA Connections and Sessions ............................ 195  
Setting Up ICA Connections .............................................. 196  
Using Citrix Connection Configuration .................................... 196  
Adding ICA Connections .................................................. 197  
Adding Asynchronous ICA Connections .................................. 198  
Configuring Session Settings for ICA Clients .......................... 200  
Precedence of Settings .................................................... 201  
Configuring ICA Connection Options .................................... 202  
Configuring Modem Callback ............................................ 202  
Configuring Direct Cable Connections .................................. 204  
Configuring Advanced ICA Connection Options ......................... 208  
Restricting Connections to Published Applications .................... 209  
Configuring ICA Encryption ............................................. 209  
Using Shadowing to Monitor ICA Sessions ............................. 209  
Enabling Shadowing on a Server ....................................... 210  
Configuring ICA Connections for Shadowing ........................... 210  
Configuring ICA Audio Settings ......................................... 212
Chapter 9  
Deploying ICA Clients to Users

Choosing a Deployment Method ........................................... 219
Delivering Applications to Users ....................................... 221
Determining the Scope of ICA Client Deployment .................. 222
Using the MetaFrame XP Components CD ............................... 223
  Pass-Through ICA Client ............................................ 224
  ICA Client Object ................................................ 224
Deploying the ICA Clients .............................................. 225
  Using Installer Packages for Client Deployment ................... 225
  Web-Based Installation ............................................ 226
  Deploying ICA Clients over a Network ............................. 226
  Deploying ICA Clients Using Diskettes ............................ 227
Updating the ICA Clients .............................................. 227
  The ICA Client Update Process ................................... 228
Configuring the Client Update Database ............................... 229
  Using the Client Update Configuration Utility ..................... 229
  Creating a New Client Update Database ............................ 230
  Specifying a Default Client Update Database ....................... 230
  Configuring Default Client Update Options ......................... 231
  Adding ICA Clients to the Client Update Database ............... 233
  Removing an ICA Client from the Client Update Database ...... 235
  Changing the Properties of an ICA Client in the Database ..... 235
ICA Client Deployment Practices ....................................... 236
  Manufacturing Enterprise .......................................... 237
  Regional Bank .................................................... 237
  Application Service Provider ....................................... 238
  Insurance Company ................................................ 239
## Chapter 10 Making Information Available to Users

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Deciding How Users Access Information</td>
<td>242</td>
</tr>
<tr>
<td>Managing Users’ Access to Information with Content Publishing and Content Redirection</td>
<td>243</td>
</tr>
<tr>
<td>Publishing Applications and Content</td>
<td>244</td>
</tr>
<tr>
<td>User Access to Published Applications</td>
<td>245</td>
</tr>
<tr>
<td>Administrative Control of Applications</td>
<td>246</td>
</tr>
<tr>
<td>Using Published Applications</td>
<td>247</td>
</tr>
<tr>
<td>Configuring User Access to Applications</td>
<td>248</td>
</tr>
<tr>
<td>Procedures for Publishing Applications</td>
<td>249</td>
</tr>
<tr>
<td>Associating Published Applications with File Types</td>
<td>250</td>
</tr>
<tr>
<td>Passing Parameters to Published Applications</td>
<td>253</td>
</tr>
<tr>
<td>Creating Files for Application Launching and Embedding</td>
<td>254</td>
</tr>
<tr>
<td>Removing Published Applications</td>
<td>255</td>
</tr>
<tr>
<td>Configuring Content Redirection</td>
<td>255</td>
</tr>
<tr>
<td>Redirecting Content from Client to Server</td>
<td>255</td>
</tr>
<tr>
<td>Redirecting Content from Server to Client</td>
<td>256</td>
</tr>
<tr>
<td>Publishing Content</td>
<td>258</td>
</tr>
<tr>
<td>Publishing Content to be Opened with Applications Published on MetaFrame Servers</td>
<td>258</td>
</tr>
<tr>
<td>Publishing Content to be Opened with Applications on Local Client Devices</td>
<td>259</td>
</tr>
<tr>
<td>Publishing Content on MetaFrame XP Servers</td>
<td>260</td>
</tr>
<tr>
<td>Setting CPU Priority Levels for Applications</td>
<td>261</td>
</tr>
<tr>
<td>Assigning CPU Priority Levels to Applications</td>
<td>262</td>
</tr>
</tbody>
</table>

## Chapter 11 Managing Users and ICA Sessions

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Controlling User Logons</td>
<td>265</td>
</tr>
<tr>
<td>Controlling User Connections</td>
<td>266</td>
</tr>
<tr>
<td>Limiting Total Connections in a Server Farm</td>
<td>267</td>
</tr>
<tr>
<td>Limiting Application Instances</td>
<td>267</td>
</tr>
<tr>
<td>Configuring Connection Control Settings</td>
<td>268</td>
</tr>
<tr>
<td>Logging Connection Control Events</td>
<td>270</td>
</tr>
<tr>
<td>Monitoring and Managing ICA Sessions</td>
<td>271</td>
</tr>
<tr>
<td>Viewing Information about ICA Sessions</td>
<td>271</td>
</tr>
<tr>
<td>Using Session Management Commands</td>
<td>273</td>
</tr>
</tbody>
</table>
Reconnecting ICA Sessions Automatically ............................... 276
   How Automatic Reconnection Works ................................. 277
   Security in Automatic Reconnection ............................... 277
   Configuring Reconnection Settings ............................... 278
   Setting Up ICA Connections for Auto Client Reconnect ............ 278
   Logging Reconnection Events ........................................ 280
Creating and Applying User Policies .................................. 281
   Prioritizing Policies .............................................. 283
Shadowing ICA Sessions .................................................. 284
   Configuring User-to-User Shadowing ............................... 286
Monitoring Performance of Sessions and Servers ......................... 288

Chapter 12  Managing Printers for ICA Clients
Overview of Printing with MetaFrame XP .............................. 291
   Client Printing in ICA Sessions ..................................... 292
   Printing Configuration Scenarios ...................................... 293
Printer Management Features .......................................... 295
   Using the Printer Management Node .................................. 295
   Using the Servers Node ............................................... 298
Setting Up Network Printers for ICA Client Users ...................... 299
Installing and Replicating Printer Drivers ............................ 300
   Setting Up Automatic Replication of Printer Drivers ............... 301
   Mapping Printer Drivers .............................................. 302
   Managing Drivers for Client Printers ............................... 302
Configuring Auto Creation of Client Printers ......................... 303
   Auto Creation for DOS and WinCE Clients ......................... 303
   Auto Creation for Other Clients ..................................... 304
   Auto Creation and Citrix Connection Configuration ................ 305
Using MetaFrame XP Universal Printing ................................ 306
   Client Printing with the Universal Driver ......................... 306
Specifying Printer Drivers for Client Printing ....................... 308
   Automatically Installing Native Drivers ............................ 308
Limiting Printing Bandwidth in ICA Sessions ......................... 309

Appendix A  MetaFrame XP Commands ........................................ 311
   ACRCFG .......................................................... 313
   ALTADDR .......................................................... 316
   APP ............................................................. 318
<table>
<thead>
<tr>
<th>Appendix B</th>
<th>Customizing MetaFrame Setup</th>
<th>367</th>
</tr>
</thead>
<tbody>
<tr>
<td>Creating Transforms</td>
<td>368</td>
<td></td>
</tr>
<tr>
<td>Creating Administrative Installations</td>
<td>374</td>
<td></td>
</tr>
<tr>
<td>MetaFrame Setup Property Names and Values</td>
<td>375</td>
<td></td>
</tr>
<tr>
<td>Appendix C</td>
<td>Glossary</td>
<td>389</td>
</tr>
<tr>
<td>Index</td>
<td>399</td>
<td></td>
</tr>
</tbody>
</table>
Welcome

The MetaFrame XP suite of products provides integrated management capabilities for system administrators, along with ease of use and productivity enhancements for end-users who access applications on MetaFrame XP servers using Citrix ICA Clients.

This chapter describes the documentation provided with MetaFrame XP and additional resources for you to find more information about MetaFrame XP and related MetaFrame XP products.

**Important** Before you install MetaFrame XP, read SP3-FR3_readme.txt, which is in the root directory of the MetaFrame XP server CD. For information about new features in MetaFrame XP and feature releases, see “Introduction to MetaFrame XP Server” on page 19.

Citrix provides a variety of information resources online, including a complete product documentation library, documentation updates, and technical articles on the Citrix Web site at http://www.citrix.com. For more information, see “Citrix on the World Wide Web” on page 17.
MetaFrame XP Documentation

The MetaFrame XP documentation includes electronic manuals and online application help.

The documentation included with MetaFrame XP is available in the Docs directory on the MetaFrame XP CD-ROM. Documentation for ICA Client software is available on the Components CD-ROM.

Documentation for additional management tools and features that are included with MetaFrame XPe is on the Components CD-ROM. Some of this documentation is also in the Docs directory on the MetaFrame XP CD-ROM.

Important additional documentation for Citrix MetaFrame XP components is available from the Product Documentation page in the Support area of the Citrix Web site at www.citrix.com/support. For example, Advanced Concepts for MetaFrame XP is a manual that provides system sizing, deployment, configuration, optimization, and troubleshooting information, which supplements the MetaFrame XP Server Administrator’s Guide.

On a MetaFrame XP server, documentation is installed in the Documentation folder. You can display the contents of this folder by choosing Programs > Citrix > Documentation from the Start menu.

The following documentation is included with MetaFrame XP in Adobe PDF format:

- This manual, the MetaFrame XP Server Administrator’s Guide, provides conceptual information and procedures for system administrators who install, configure, and maintain MetaFrame XP Server for Windows. To get the most out of the guide, review the table of contents to familiarize yourself with the topics included in the book.

- The readme file and readmes for feature releases contain last minute updates, corrections to the documentation, and a list of known problems. These files are in the root directory of the MetaFrame XP CD-ROM.

- The Web Interface for MetaFrame XP Administrator’s Guide tells administrators how to install, configure, and customize the Web Interface for MetaFrame XP.

- The ICA Client Administrator’s Guides provide instructions for system administrators who deploy ICA Clients to end-users on various computing platforms.
This manual is available in the following locations:

- In the \Docs directory of your MetaFrame XP CD-ROM
- Installed in the Documentation folder of your MetaFrame XP server. From the Start menu, choose Programs > Citrix > Documentation.
- On the Citrix Web site at http://www.citrix.com/support; select Product Documentation. You can check the Product Documentation area of the Web site at any time for the latest updates to Citrix technical manuals. Any updates to this manual published after the release of this product will be posted there.

**Using PDF Documentation**

To access the MetaFrame XP documentation that is provided in PDF files, use Adobe Acrobat Reader 4 or later. Acrobat Reader lets you view, search, and print the documentation.


**Documentation Conventions**

MetaFrame XP documentation uses the following typographic conventions for menus, commands, keyboard keys, and items in the program interface:

<table>
<thead>
<tr>
<th>Convention</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Boldface</strong></td>
<td>Commands, names of interface items such as text boxes, option buttons, and user input.</td>
</tr>
<tr>
<td><em>Italics</em></td>
<td>Placeholders for information or parameters that you provide. For example, <em>filename</em> in a procedure means you type the actual name of a file. Italics also are used for new terms and the titles of books.</td>
</tr>
<tr>
<td><strong>UPPERCASE</strong></td>
<td>Keyboard keys, such as CTRL for the Control key and F1 for the function key that is labeled F1.</td>
</tr>
<tr>
<td>Monospace</td>
<td>Text displayed in a text file.</td>
</tr>
<tr>
<td>%SystemRoot%</td>
<td>The Windows system directory, which can be WTSRV, WINNT, WINDOWS, or other name specified when Windows is installed.</td>
</tr>
<tr>
<td>{ braces }</td>
<td>A series of items, one of which is required in command statements. For example, {yes</td>
</tr>
<tr>
<td>[ brackets ]</td>
<td>Optional items in command statements. For example, [ping] means that you can type /ping with the command. Do not type the brackets themselves.</td>
</tr>
</tbody>
</table>
Using Online Help

Online help is available for the Management Console for MetaFrame XP and the other tools that are included with MetaFrame XP.

You can access online help from the Help menu of each program; the program must be running for you to view its online help. You can use shortcuts to launch MetaFrame XP utilities and the Management Console. Shortcut icons are located in the MetaFrame XP folder. To open this folder, click the Start menu and choose Programs > Citrix > MetaFrame XP.

Online help for the Management Console is in JavaHelp format and requires the Java Run-Time Environment (JRE), which MetaFrame XP installs by default on the server. Online help for server utilities and the Windows ICA Clients is in WinHelp format, which is available by default on all Windows systems. Online help for other ICA Clients uses standard help formats for their platforms.

Citrix ICA Client software for all platforms includes online help for using applications and configuration settings. Help is available from Help menus or Help buttons in the ICA Clients.

Providing Feedback about this Guide

We strive to provide accurate, clear, complete, and usable documentation for MetaFrame XP products. If you have any comments, corrections, or suggestions for improving our documentation, we want to hear from you.

You can send e-mail to the documentation authors at documentation@citrix.com. Please include the product name, product version number, and the title of the document in your message.

Finding Information about Windows Servers

Most compatibility guidelines for Windows Server 2003 and Windows 2000 Servers can be applied to Citrix MetaFrame XP because MetaFrame XP is designed to run with these products.
Important MetaFrame XP Feature Releases 2 and higher do not operate on Windows NT Server 4.0, Terminal Server Edition.

For example, MetaFrame XP supports the deployment of Win32, Win16, DOS, OS/2 1.x (text only), and POSIX applications. The ICA technology included in MetaFrame XP extends the capabilities of Windows servers and, in some cases, requires additional setup and configuration for best application performance.

Instructions for installing and using Windows servers are included in the Microsoft documentation included in your Windows package and can also be found on the Microsoft Web site at http://www.microsoft.com.

Citrix on the World Wide Web

The Citrix Web site is at http://www.citrix.com. The site offers a variety of information and services for Citrix customers and users.

From the Citrix home page, you can access Citrix technical support services and other information designed to assist MetaFrame XP administrators.

The following are some of the resources available on the Citrix Web site:

Citrix Product Documentation Library. The library, which contains the latest documentation for all MetaFrame XP products, is at http://www.citrix.com/support (select Product Documentation). You can download updated editions of the documentation that ships with MetaFrame XP products, as well as supplemental documentation that is available only on the Web site.

Citrix ICA Clients. Downloadable Citrix ICA Clients for all supported platforms are available from http://www.citrix.com/download.


Software downloads. An FTP server provides access to the latest service packs, hotfixes, and utilities.

Online knowledgebase. The online Solution Knowledge Base contains an extensive collection of application notes, technical articles with answers to frequently answered questions, troubleshooting tips, and white papers. The Knowledge Base is available at http://www.citrix.com/support.

Discussion forums. The interactive online Solution Forums provide outlets for discussion of technical issues with other Citrix users.
Education. Information about programs and courseware for Citrix training and certifications is available from http://www.citrix.com/training/.

Contact information. The Web site provides contact information for Citrix offices, including the worldwide headquarters and headquarters for European, Asia Pacific, and Japan operations.

Developer network. The Citrix Developer Network (CDN) is at http://www.citrix.com/cdn. This open-enrollment membership program provides access to developer toolkits, technical information, and test programs for software and hardware vendors, system integrators, ICA licensees, and corporate IT developers who incorporate Citrix computing solutions into their products.

SDKs. The Citrix Server Software Development Kit (SDK) is available for free from www.citrix.com/cdn. Most of the operations that you can perform through Citrix GUI tools can be scripted by using the MetaFrame XP Server SDK. The SDK also lets programmers customize most aspects of MetaFrame XP.
Introduction to MetaFrame XP Server

This chapter introduces MetaFrame XP Server and MetaFrame XP feature releases and includes descriptions of new features in the latest MetaFrame XP feature release.

Overview of Server-Based Computing

Heterogeneous computing environments are a fact of life in the enterprise today. Computing infrastructures typically are built around incompatible parts, including an installed base of various client devices (PCs, terminals, network computers, portables), different operating systems, multiple network protocols, and various types of network connections.

Regardless of differences in computing environments, enterprises need to make applications available to all of their users. MetaFrame XP can bridge differences in computing environments. MetaFrame XP allows organizations to keep their desktops of choice and provide the best application fit for users and the enterprise.

The MetaFrame XP application server suite of software and Independent Computing Architecture (ICA) Client software are designed to meet the needs of all types of businesses. Any organization whose customers require robust, easily managed, and cost-effective delivery of Windows applications to a variety of client devices can greatly benefit from using the MetaFrame XP suite.

Server-based computing is a logical, efficient paradigm for today’s networking environments. Server-based computing helps organizations simplify application deployment and administration, thereby reducing the total cost of ownership of their application services.
Components of Server-Based Computing

The components and technologies that enable server-based computing include the MetaFrame XP application server suite, ICA Client software, the ICA protocol, and Independent Management Architecture (IMA), the foundation layer that unifies server-based computing solutions.

Server-based computing is built on several key components:

**Multiuser operating system.** Server-based computing requires an operating system that allows multiple concurrent users to log on and run applications in separate, protected sessions on a single server. MetaFrame XP runs on the Windows server operating system families. In these server operating systems, MultiWin technology licensed from Citrix provides the multiuser capabilities.

---

**Note** MetaFrame XP with Feature Release 3 is supported on Windows 2000 Server and Windows Server 2003 operating systems. MetaFrame XP with Feature Release 2 is supported only on Windows 2000 Server operating systems. MetaFrame XP, Feature Release 1 is supported on Windows 2000 Server and Windows NT Server 4.0, Terminal Server Edition.

---

**MetaFrame XP Server software.** MetaFrame XP Server is the application server component of Citrix’s server-based computing solutions. MetaFrame XP Server incorporates Citrix’s ICA protocol. The ICA protocol separates an application’s logic from its user interface, so that only keystrokes, mouse clicks, and screen updates (with required data such as sound) are sent across the network.

**Citrix ICA Clients.** Users access applications running on MetaFrame XP servers using ICA Client software installed on their client devices. ICA lets virtually any type of client device access applications over any type of network connection, including LAN, WAN, dial-up, and direct asynchronous connections. Because ICA does not download applications to client devices (as in the Network Computing architecture), application performance is not limited by bandwidth or device performance. See “Independent Computing Architecture and ICA Clients” on page 22 for more information.

---

Overview of MetaFrame XP Server Farms

MetaFrame XP server farms provide you with a flexible and robust way of deploying applications to ICA Client users. A MetaFrame XP server farm is a group of MetaFrame XP servers managed as a single entity. Servers share some form of physical connection. In addition, the servers in the server farm share a single data store.
Note  Servers running MetaFrame 1.8 and earlier versions can be grouped in server farms for application publishing and centralized administration. However, MetaFrame 1.8 and earlier versions do not use a centralized data store for a server farm. MetaFrame XP servers cannot join a server farm running earlier versions of MetaFrame. For information about interoperability of MetaFrame XP with MetaFrame 1.8 servers, see “Interoperability with MetaFrame 1.8” on page 100.

MetaFrame XP uses the data store to centralize configuration information for a server farm in one location. The data store maintains information about the servers, applications, and MetaFrame XP administrators in the server farm. Creation of a data store and connection to the data store by each server is a part of MetaFrame XP setup.

Independent Management Architecture (IMA)

MetaFrame XP incorporates the advanced MetaFrame XP server communications and management foundation, the Independent Management Architecture (IMA). The integration of the MetaFrame XP application server software with IMA is central to the enhanced functionality of MetaFrame XP and the scalability of Citrix’s server-based computing solutions.

IMA is a unified, enterprise-wide platform for installation, management, maintenance, support, and security for your organization’s server-based computing and application hosting services. It is both an architectural model and a protocol for server-to-server communications. IMA is constructed on a collection of core subsystems that define and control execution of Citrix products.

IMA enables MetaFrame XP servers to be arbitrarily grouped into server farms that do not depend on the physical locations of the servers. IMA allows MetaFrame XP servers to be in a single server farm even if the servers are on different network subnets.

With MetaFrame XP for Windows servers and the extensible Citrix IMA foundation, organizations gain a wide range of enterprise management and scalability features and options:

- Central administration of MetaFrame XP and other MetaFrame servers
- Centralized data store for all MetaFrame XP farm configuration data
- Centralized license management and pooling without license gateways
- ICA Client discovery of published applications without UDP broadcasts
- Logging of shadowing events
- Simple Network Management Protocol (SNMP) support
- Auditing of administration activity
While IMA and MetaFrame XP provide significant enhancements that facilitate enterprise application hosting, both MetaFrame XP and IMA support the current functionality of all existing ICA Client software from Citrix and will operate with an installed base of ICA Clients.

In addition to the Management Console for MetaFrame XP, several Windows-based management utilities are included with MetaFrame XP. These utilities provide management and configuration features that are independent of the IMA system.

As the size of an organization increases from dozens to hundreds to thousands of users, additional MetaFrame XP servers can be added to the server farm. With IMA, MetaFrame XP installations can scale to multi-site, enterprise-level server-based computing scenarios, while administrators maintain complete control from any location.

**Independent Computing Architecture and ICA Clients**

MetaFrame XP provides server-based computing to local and remote users through the Independent Computing Architecture (ICA) developed by Citrix.

ICA is the foundation of Citrix server-based computing with MetaFrame XP and ICA Client software. In simplified terms, the ICA protocol transports an application’s screens from a MetaFrame XP server to ICA Client users, and returns the users’ input to the application on the server.

As an application runs on a MetaFrame XP server, MetaFrame XP intercepts the application’s display data and uses the ICA protocol to send this data (on standard network protocols) to the ICA Client software running on the user’s client device. When the user types on the keyboard or moves and clicks the mouse, the ICA Client sends this data to the application on the MetaFrame XP server.

The Citrix ICA protocol provides advanced capabilities and enhanced performance with Windows terminal services. ICA delivers high performance on high- and low-bandwidth connections. It requires minimal client workstation capabilities and includes error detection and recovery, encryption, and data compression.

**Citrix ICA Clients**

Citrix ICA Client software lets users connect to MetaFrame XP servers and access applications. The ICA Client extends the reach of Windows, Java, and UNIX-based applications to virtually any client platform or device, including: 286, 386, 486, and Pentium-based PCs, Windows-based terminals, network computers, wireless devices, ICA-based information appliances, RISC-based systems, PowerPCs, UNIX based computers, and X-based devices.

ICA clients are available for Windows, Macintosh, UNIX, Linux, EPOC, Windows CE, DOS, and Java operating systems, as well as for Web browsers that use the ActiveX control or Netscape plug-in.
Overview of the MetaFrame XP Family

MetaFrame XP is available in three tailored solutions:

- MetaFrame XPs is designed to give businesses outstanding performance from applications running on a central server.
- MetaFrame XPa is designed with the small to medium business in mind. A MetaFrame XPa license enables all of the features of MetaFrame XPs and also includes load balancing functionality.
- MetaFrame XPe is designed for single-point control of servers, licenses, and resources in large organizations and multinational corporations. A MetaFrame XPe license enables all of the features of MetaFrame XPa and also provides system monitoring and analysis, application packaging and delivery, and integration with third-party SNMP management consoles.

These solutions enable you to install and license only those features and components that you need on a specific server.

For more details about the features and components included in each family level of MetaFrame XP, see Getting Started with MetaFrame XP on the MetaFrame XP Server CD.

Features of MetaFrame XP for Windows

Major features of MetaFrame XP, including IMA and the Management Console, are discussed earlier in this chapter. This section describes other features of MetaFrame XP.

Application Server Features

**Application publishing.** Publishing an application on a MetaFrame XP server makes it available to ICA Client users (with proper authorization). You can publish applications across multiple servers in the server farm. With the optional Load Manager component, you can balance connections from ICA Client users to connect users to the least-loaded MetaFrame XP servers.

**Client Device Licensing.** A user can establish multiple sessions to multiple servers while consuming only a single pooled connection license count for each session.
Automatic ICA Client update. MetaFrame XP lets you automate distribution of updated versions of Citrix ICA Client software to client devices. After you install the latest ICA Client software on the server, you can schedule the download and installation of the updated software to client devices. For more information, see “Deploying ICA Clients to Users” on page 219.

Security. MetaFrame XP incorporates multilevel system security and 128-bit data encryption. MetaFrame XP administrator accounts can be configured with read-only or read-write access to Management Console for MetaFrame XP for management of MetaFrame XP server farms. During MetaFrame XP installation, you can disable the ability to shadow ICA Client sessions, or you can allow shadowing but require logging of shadowing events to create an audit trail.

TCP/IP port setting. You can configure Citrix ICA packets to be compatible with many popular TCP/IP firewall products. For more information, see the ALTADDR command in “Command Reference,” Appendix A.

SpeedScreen. SpeedScreen reduces the transmission of frequently repainted screens to reduce bandwidth consumption. SpeedScreen latency reduction provides instant mouse-click feedback and local text echo. These features increase perceived performance of ICA sessions over high-latency connections. SpeedScreen latency reduction is not available in the Japanese version of MetaFrame XP.

Application management. MetaFrame XP enables you to manage and extend the reach of enterprise applications with tools such as Application Launching and Embedding (ALE) and application publishing. With ALE, you can extend applications across the Web without programming. Application publishing lets ICA Client users access applications as simply as other resources on the network. You can deploy and manage multiple servers and applications from a single point.

Citrix ICA Client Features

Citrix ICA Clients share many features for connecting to MetaFrame XP servers. Some features are available on particular ICA Clients. For detailed information about supported features, see the ICA Client Administrator’s Guide for each client you use.

Program Neighborhood. Program Neighborhood — the user interface that allows users to browse for application sets from client devices running 32-bit Windows desktop operating systems — gives you complete application control by publishing server-based applications to the local desktops. With Program Neighborhood, server-based applications can be pushed to the client device, integrated into the local desktop, or pushed directly to the Start menu.
TAPI support. The ICA Client for Win32 provides TAPI support for dial-up connections. Citrix ICA Clients for DOS and Win16 can interpret Windows 9x and Windows 2000 modem configuration files into legacy Ini files to ensure optimum performance for dial-up users.

International keyboard support for Web browsers. Users worldwide can use the Citrix ICA Clients with Internet Explorer and Netscape, current versions of which support international keyboard layouts.

Client device mapping. Users can transparently access local printers and disk drives. Drive letters on the MetaFrame XP server are configurable so client devices can keep their drive letters. Long filenames are supported. Any printers detected when you connect to a MetaFrame XP server are automatically mapped for use with the applications users run on the server. Client printers can be browsed and connected to in the same way as network printers (Windows, WinCE, and DOS Clients).

COM port mapping. The ICA Client COM port redirector lets ICA Client users (DOS, Win16, and Win32 platforms) use most peripherals that connect to serial ports as if they were connected to a COM port on the MetaFrame XP server.

Windows clipboard integration. Users can cut and paste data between ICA sessions and local applications using the Windows Clipboard.

Audio support. MetaFrame XP provides audio support for most ICA Clients. You can use compression to maximize bandwidth utilization. ICA supports audio through Sound Blaster 16-compatible sound hardware in DOS and Windows client devices.

Disk caching and data compression. These options increase performance over low-speed asynchronous and WAN connections. Disk caching stores frequently used application images (such as icons and bitmaps) locally, increasing performance by avoiding retransmission of locally cached data. Data compression reduces the amount of data sent over the communications link to the client device.

Seamless windows support. Certain ICA Clients support the seamless integration of local and remote applications on the local desktop. Configuring an ICA connection for seamless windows lets users switch among local and remote applications with keyboard controls or the local taskbar. Seamless windows connections also support remote application icons on the local desktop, and tiling and cascading between local and remote Windows applications.

Business recovery. ICA Clients support multiple site addresses (for primary and hot backup, for example) for the same published application name. This feature helps assure consistent connections to published applications in the event of server disruptions.
Client print manager. Users can define which client printers can be configured on their client devices. This feature provides a means to store printer properties on a per-client-device basis while simplifying printer configuration for non-Windows clients.

Multi-monitor support. The ICA Win32 Client supports the multi-monitor features of Microsoft Windows 98, Windows 2000, and Windows XP clients. It also supports the virtual desktop feature provided by some graphics cards for Windows 95 and Windows NT 4.0.

Panning and scaling. If the ICA session is larger than the client computer’s desktop, you can pan the ICA session window around the full session desktop. Scaling allows you to view more of the ICA session at one time without panning by shrinking the perceived size of the ICA session. See the ICA Client Administrator’s Guide for instructions about using this feature on a particular ICA Client.

MetaFrame XP Feature Releases

Citrix periodically makes available feature releases in between major platform releases of MetaFrame XP.

To use the new features included with feature releases, you must install and activate feature release licenses. For more information about MetaFrame XP and feature release pricing and availability, see the Citrix Web site at http://www.citrix.com.

Features Included in Feature Release 3

With Feature Release 3, MetaFrame XP includes support for the Web Interface and Web Interface Extension for MetaFrame XP, and Secure Gateway 2.0. For information about these products, see the documentation in the corresponding Docs directories on the Components CD included with MetaFrame XP, Feature Release 3.

Features included in Feature Release 2 and Feature Release 1 are installed with MetaFrame XP for Feature Release 3.

MetaFrame XP Features Name Changes

With Feature Release 3, many MetaFrame XP components are integrated into a MetaFrame XP suite of applications. The following MetaFrame XP feature names have been changed to reflect this integration:

- NFuse Classic is now called the Web Interface for MetaFrame XP.
- Enterprise Services for NFuse is now called the Web Interface Extension for MetaFrame XP.
The Citrix Management Console is now called the Management Console for MetaFrame XP.

Citrix Secure Gateway is now called the Secure Gateway for MetaFrame.

MetaFrame XP

MetaFrame XP with Feature Release 3 includes the following new features and enhancements. You must install the appropriate Feature Release 3 licenses to enable these features.

**Important** New features in Feature Release 3 are not available when a server farm operates in mixed mode for interoperability with MetaFrame 1.8.

Support for Microsoft Windows Server 2003. All family levels of MetaFrame XP with Feature Release 3 - MetaFrame XPc, MetaFrame XPa, and MetaFrame XPs - run on Microsoft’s latest version of the Windows server operating system.


Support for SQL Server 2000 Database Engine (MSDE). You can use SQL Server 2000 Desktop Engine (MSDE) to host the MetaFrame XP server farm’s data store. MSDE is suitable for use in small MetaFrame XP farms.

For more information about using MSDE to host the MetaFrame XP server farm’s data store, see “Choosing a Database for the Data Store” on page 50 and “Installing MetaFrame XP” on page 105.

Enhanced Printing Capabilities. MetaFrame XP with Feature Release 3 includes the following enhancements to printing.

- Color and high-resolution printing with MetaFrame XP Universal Printing. Users printing with universal printer drivers can now print to color and high-resolution printers (up to 600 dots per inch).
- Automatic installation of allowed print drivers for auto-created network printers. Print drivers are automatically installed for network printers.

For more information about the enhanced printing capabilities included in MetaFrame XP with Feature Release 3, see “Managing Printers for ICA Clients” on page 291.
**SpeedScreen Browser Acceleration.** SpeedScreen Browser Acceleration introduces major performance improvements for users connecting to applications that embed JPEG and GIF images within MSHTML pages. Supported applications are Internet Explorer (Version 5.5 or later), Microsoft Outlook, and Outlook Express published on a MetaFrame XP server.

**Note** Users must be running Version 7.0 of the ICA Win32 Client, with a minimum connection color depth of 16-bit, to realize the SpeedScreen Browser Acceleration improvements.

SpeedScreen Browser Acceleration requires less bandwidth and allows users running the supported applications to interact with the browser while graphically-rich pages or large images are being downloaded. When the SpeedScreen Browser Acceleration feature is enabled, the user’s browsing experience is improved with the following functionality:

- **Background image delivery.** Users can now click Back and Stop while images are being downloaded from Web sites.
- **Progressive drawing.** JPEG images begin to appear in the browser before they are completely downloaded, allowing users to interact with them without having to wait until they are finished downloading.
- **Responsive scrolling.** Users can now scroll Web pages before any image content is served. Images continue to be downloaded while users interact with the browser.

You can enable SpeedScreen Browser Acceleration for individual MetaFrame servers or for an entire MetaFrame XP server farm. For more information about enabling SpeedScreen Browser Acceleration, see “Improving Responsiveness with SpeedScreen Browser Acceleration” on page 193 and the online Help for the Management Console for MetaFrame XP.

**Simplified License Activation.** Run the mlicense command line utility to add, activate, and back up multiple electronic licenses in your server farm. For more information about using mlicense, see “MLICENSE” on page 351.

**ICA Program Neighborhood Agent as the Pass-Through Client.** You can choose to install the ICA Program Neighborhood Agent on the MetaFrame server during MetaFrame Setup. You can allow users to connect to the server desktop and use the functionality of the Program Neighborhood Agent.

For more information about installing the ICA Pass-Through Client on the MetaFrame XP server, see “Installing the ICA Pass-Through Client” on page 114.
Management Console for MetaFrame XP Enhancements. The Management Console includes the following usability improvements. See the console’s online Help for more information about configuration settings and options.

- **Improved navigation.** In lists of users and groups, you can navigate to items by typing the first few letters of the user or group name. The total count of items in a list is displayed in the console’s task bar. If you change the view in the console to Details, this view remains until you close the console or change to another view.

- **Summary of server farm information.** Aggregate information about a server farm is displayed on a farm summary page. In the Management Console for MetaFrame XP, right-click the server farm and select **Properties.** Click Information in the left pane.

- **ICA Keep-Alive settings.** You can now set intervals for ICA Keep-Alives for your entire MetaFrame XP server farm or for select servers. Right-click your farm or a server in the farm and select **Properties.** Click ICA Keep-Alive in the left pane.

- **Support for Sun Java Runtime Environment Version 1.4.1.** The Management Console for MetaFrame XP requires Version 1.4.1 of the JRE. If Version 1.4.1 of the JRE is not detected when installing the console, it is installed.

Remote server access and management. You can connect to MetaFrame XP servers or launch ICA sessions from within the Management Console for MetaFrame XP. Right-click the server to which you want to connect and select one of the available options. You can connect directly to the server’s desktop or to the server’s published desktop, or you can connect to the server’s console if you’re running Windows Server 2003.

MetaFrame XPe Components

The optional components of MetaFrame XPe include the following new features and enhancements.

Resource Manager

Resource Manager includes the following new features and enhancements. Resource Manager is included with MetaFrame XPe. For more information about the new features in Resource Manager, see the *Resource Manager Administrator’s Guide* in the Docs directory on the MetaFrame XP server CD.

Improved Billing. Fees are now arranged into Fee Profiles. Each fee profile contains a set of fee rates and a currency symbol. A fee profile can be used by one or more cost centers when producing a billing report.
You can create a custom MetaFrame XP administrator account that allows access to billing only. Use the delegated administration feature of MetaFrame XP to configure the custom account.

**Apply to Folder Support.** When making changes to metric settings or application settings across servers, you can apply to a folder structure, previously defined in the Management Console for MetaFrame XP. Selecting servers is now much more intuitive.

**SMTP Mail Support.** You can configure Resource Manager to send alerts using Simple Mail Transfer Protocol (SMTP). SMTP offers ease of setup and does not require an email package to be installed locally.

**User-definable Installation.** You can specify where the local Resource Manager database is installed during Setup. You can set up the storage elements of the local database.

**Improved Snapshot Report.** More problem solving information is now displayed in the snapshot report. The report shows the processes using more than 5% of the processor or memory and shows highest resource usage by user.

**Improved Server Restarting.** You can prevent users from logging on for a period of time before the server restarts. You can also schedule servers to restart in a staggered manner in a definable time period.

**Report Printing.** Print reports that you generate in Resource Manager, including billing reports. You can scale a report to fit on a particular number of pages, or to a particular percentage of its normal size.

**Summary Database Folders and Zones.** You can produce Summary Database reports on groups of servers that you previously defined using the Management Console for MetaFrame XP. You can monitor and assess the performance of the server groups, allowing new hardware requirements to be addressed.

**Improved SNMP Traps.** To improve the level of detail in SNMP alerts, the single “trapAlert” SNMP trap for Resource Manager has been replaced with five new traps.

**Alert on Yellow.** You can configure Resource Manager to raise an alert when a yellow threshold is crossed, allowing you to proactively fix problems before they arise. Configure alerts using a new, improved interface.
MOM and WMI

MetaFrame XPe includes support for the management technology that integrates the monitoring of MetaFrame XPe servers and server farms into Microsoft Operations Manager (MOM) 2000, the latest network and server management tool from Microsoft.

The MetaFrame XP Management Pack for MOM is used in conjunction with the Microsoft Windows Management Instrumentation (WMI) Provider for MetaFrame XP, an agent installed on each MetaFrame XP server. Use the Management Pack for MOM and the WMI Provider to monitor the health and performance of MetaFrame XP servers and underlying Microsoft Windows servers using the MOM environment.

For more information about using MetaFrame XP with MOM and WMI, see the Administrator’s Guide for the WMI Provider for MetaFrame XP in the Docs directory on the MetaFrame XP Server CD.

MetaFrame XP Management Pack for MOM 2000. The MetaFrame XP Management Pack is a plug-in for MOM that you can use to monitor the health and availability of MetaFrame XPe servers and server farms. MOM provides real-time event and performance monitoring and includes an extensive knowledge base, with links to Citrix Knowledge Base articles and other sources of information.

WMI Provider for MetaFrame XP. Windows Management Instrumentation (WMI) is the standard management infrastructure included as part of Microsoft Windows 2000 and Windows XP. The WMI Provider for MetaFrame XP supplies the information about MetaFrame XPe servers and server farms that is displayed in the MetaFrame XP Management Pack for MOM.

You must install the WMI Provider on each MetaFrame XP server you want to monitor with MOM. You install the WMI Provider when you install MetaFrame XPe.

ICA Clients

MetaFrame XP with Feature Release 3 includes Version 7.0 of the ICA Win32 and ICA Java Clients, and Version 6.30 of the ICA Macintosh Client, developed specifically for the Mac OS X operating system.

For more information about the ICA Clients described below, see the Administrator’s Guides for the ICA Clients in the ICAClientDoc directory on the MetaFrame XP Components CD.

ICA Win32 Client

Version 7.0 of the ICA Win32 Client includes the following new features and enhancements.
Custom Window Shapes. The ICA Win32 Client now supports custom window shapes. This improvement provides the appearance of rounded corners in seamless application windows to integrate more cleanly into Windows XP-themed desktops, such as the default Windows XP theme.

Minimal Installation ICA Win32 Web Client. Core ICA Win32 Client functionality is available in an ActiveX control. The ActiveX control is packaged into a .Cab file (wficac.cab) and can be used with Internet Explorer 5.0 and higher. Use this client in situations where a smaller download is required, and where options such as audio or COM port mapping are not required.

The ICA Win32 Web Client is also packaged into a .Cab type file (wficat.cab). The .Cab file allows a smaller download than the self-extracting executable package for the ICA Win32 Web Client (wifcat.exe).

Program Neighborhood Agent Administrative Tool. You can configure user settings with the ICA Win32 Program Neighborhood Agent administrative tool.

Auto Client Reconnect Enhancements. The Auto Client Reconnect feature has been improved for the ICA Win32 Clients. If network problems cause a user’s session to be disconnected, the client attempts to reconnect indefinitely unless the reconnection process is cancelled by the user.

Dynamic Client Name Support. The ICA Win32 Clients now support dynamic client names. By default, the client name is set to the machine name when the client software is installed, and is updated if the machine name changes.

Certificate Revocation Checking. When connecting to a MetaFrame XP server using SSL or TLS, the ICA Win32 Clients check whether or not the server’s certificate has been revoked.

Enhanced XML Error Messages. Messages are improved to provide better information for diagnostic troubleshooting.

ICA Java Client

Version 7.0 of the ICA Java Client includes the following new features and enhancements.

Seamless Support. Includes support for seamless windows, session sharing, and the Connection Center utility.

Content Redirection. The ICA Java Client supports redirecting the opening of content from server to client.

Reconnection to Arbitrary Sized Sessions. Users can reconnect to sessions of a size different from the fixed size applet panel.
Enhanced XML Error Messages. Messages are improved to provide better information for diagnostic troubleshooting.

Smaller SSL Libraries. The smaller SSL libraries in the Java Client reduce download time.

Client Drive and Printer Mapping. Client drive and client printer mapping performance is improved.

ICA Macintosh Client (Version 6.30 for Mac OS X)

Version 6.30 of the ICA Macintosh Client is an ICA Client developed specifically for the Mac OS X operating system, providing native connectivity to MetaFrame XP servers for Macintosh users. It adheres to the new Aqua user interface features and behaviors to offer a user experience consistent with other applications running on Mac OS X.

See the Administrator's Guide for Version 6.30 of the ICA Macintosh Client for more information. This document (file name ICA_MacOSX_Guide.pdf) is on the MetaFrame XP Component CD in the ICAClientDoc directory.

Features Included in Feature Release 2

MetaFrame XP with Feature Release 2 includes the following features and enhancements. Features included in Feature Release 2 and Feature Release 1 are installed when you install Feature Release 3.

MetaFrame XP

MetaFrame XP 1.0, Feature Release 2 includes the following new features and enhancements. You must install the appropriate Feature Release 2 licenses to enable these features.

Important New features in Feature Release 2 are not available when a server farm operates in mixed mode for interoperability with MetaFrame 1.8.

Delegated administration. MetaFrame XP administrators can delegate areas of MetaFrame administration and farm management to IT staff. Administrators can assign staff members to perform specific MetaFrame farm management tasks such as managing printers, published applications, or user policies. Members of the enterprise’s IT staff can carry out their assigned tasks without being granted full access to all areas of farm management.

For more information, see “Configuring MetaFrame XP Administrator Accounts” on page 78 and “Configuring MetaFrame XP Administrator Accounts” on page 174.
User-to-user shadowing. Users can shadow other users without requiring administrator rights. Multiple users from different locations can view presentations and training sessions, allowing one-to-many, many-to-one, and many-to-many online collaboration.

For more information, see “Configuring User-to-User Shadowing” on page 286.

Smart card support. You can use smart cards with MetaFrame XP, supported ICA Clients, and the Web Interface to provide secure access to applications and data. Using smart cards with MetaFrame and the ICA Clients simplifies the authentication process while enhancing logon security. MetaFrame XP supports smart card authentication to published applications, as well as to “smart card enabled” applications such as Microsoft Outlook.

For more information, see “Using Smart Cards with MetaFrame XP” on page 97.

Content Redirection. Administrators can specify whether local or remote applications are used to open content, allowing the appropriate application to be launched to better meet the needs of the user. With Content Redirection, you gain flexibility when considering application installation and content storage locations.

Use Content Redirection to redirect application launching from:

- **Client to server.** Content, such as a file attached to an email message, that the user encounters when running a local application is opened with an application published on the MetaFrame XP server.

- **Server to client.** URL links that the user encounters when running an ICA session are opened using the locally installed Web browser.

For more information, see “Making Information Available to Users” on page 241.

Content Publishing enhancements. When you publish content using the functionality introduced in Feature Release 1 for MetaFrame XP, you can direct users to open the published content with an application published on a MetaFrame XP server with Feature Release 2. Previously, users could open published content only with locally installed players or viewer applications. Content Publishing now allows “browser only” devices that do not have locally installed applications to open content published on MetaFrame XP servers. This capability is supported only when users connect to published content through the Web Interface.

For more information, see “Making Information Available to Users” on page 241.

User Policies. With User Policies, you can apply select MetaFrame XP settings, including shadowing permission settings, printer autocreation settings, and client device mapping settings, to specific users or user groups. Using policies, you can tailor your environment at the user level. User Policy settings override all other MetaFrame XP and Terminal Services settings.

For more information, see “Creating and Applying User Policies” on page 281.
Management Console for MetaFrame XP enhancements. The Management Console for MetaFrame XP now includes the following enhancements:

- **Better integration with Active Directory.** When you add users to console areas such as published applications or user policies, the interface reflects the hierarchical relationships of the Active Directory Organizational Unit structure. This tighter integration allows improved usability and faster enumeration. User objects are not enumerated until their host container is expanded.

- **Pass-through authentication.** MetaFrame XP administrators can log on to the console using the credentials of the local user, eliminating the need to enter credentials each time.

- **Ticketing.** When using the pass-through authentication logon method, MetaFrame XP administrator credentials are not passed over the wire. Ticketing provides secure and confidential authentication.

- **Search capability.** You can search your published applications, user policies, and autocreated printers for users or user groups.

Windows Installer support. MetaFrame XP, MetaFrame XP feature releases, and many MetaFrame XP components are available in Windows Installer packages (.msi files). All family levels of MetaFrame XP (MetaFrame XPs, XPa, or XPe) are installed from a single setup program and a single CD-ROM.

For more information about MetaFrame XP Setup, see “Installing MetaFrame XP” on page 105 and “Customizing MetaFrame Setup” on page 367.

IBM DB2 support. You can now use IBM DB2 for your farm’s data store. MetaFrame XP supports IBM DB2 Universal Database Enterprise Edition Version 7.2 with FixPak 5.

For more information, see “Choosing a Database for the Data Store” on page 50 and “Installing MetaFrame XP” on page 105.

Printer management enhancements. Enhancements to printer management allow you to:

- Set printing preferences for autocreated printers, including paper size and copy count
- Refresh users’ printer settings each time they log on to an ICA session
- Choose to save or purge the print queue when users log off
- Configure published applications to launch without waiting for all printers to be created

For more information, see the online Help for the Printers node in the Management Console for MetaFrame XP.
**Citrix Web Console enhancements.** The Citrix Web Console now includes searching and filtering capabilities and an improved layout, including static buttons.

**Transport Layer Security (TLS) encryption.** MetaFrame XP now includes support for TLS, the latest cryptographic security protocol. Client-to-server communication now passes through TLS and uses encryption modules certified with Federal Information Processing Standard (FIPS) 140 requirements.

For more information, see “Setting up Citrix SSL Relay” on page 162.

**MetaFrame XPe Components**

The optional components of MetaFrame XPe include the following new features and enhancements.

**Installation Manager**

Enhancements to the application packaging and delivery function in Installation Manager allow you to:

- Group packages and stagger their delivery across MetaFrame XP server groups
- Configure multiple share points for WAN package delivery
- Add Windows Installer patch files to existing packages

For more information, see the *Installation Manager Administrator’s Guide* in the Docs directory on the MetaFrame XP Server CD-ROM.

**Resource Manager**

Enhancements to Resource Manager allow to you:

- Collect performance, session, and application data in a centralized database for the entire MetaFrame XP farm
- Produce reports, including billing reports for CPU usage or connection time, based on predefined templates created with Crystal Reports

For more information, see the *Resource Manager Administrator’s Guide* in the Docs directory on the MetaFrame XP Server CD-ROM.

**ICA Clients**

With the release of Version 6.30, the ICA Clients include the following new features and enhancements. Version 6.30 of the ICA Clients is included with MetaFrame XP with Feature Release 2.
Roaming User Reconnect. Users can reconnect to a disconnected session with their user name rather than the device name. This functionality is supported by the full ICA Win32 Program Neighborhood Client, the Program Neighborhood Agent, and ICA Clients that connect to published applications through the Web Interface.

Enhanced Internet proxy support. ICA Clients support the following security enhancements.

- **Secure Proxy (HTTP/SSL Tunnel Proxy).** In addition to SOCKS proxy, ICA Clients now support Secure Proxy.
- **Proxy authentication.** ICA Clients now support proxy authentication with both SOCKS and HTTP/SSL Tunnel proxies.
- **Proxy auto-detection.** ICA Clients can now automatically detect proxy configuration by querying proxy information managed by Internet Explorer or Netscape browsers.
- **Proxy auto-configuration script interpreter.** ICA Clients can now interpret proxy auto-configuration (.Pac) JavaScript to derive the proxy configuration when this type of proxy configuration is detected.

For more information, see the *Administrator’s Guides* for the ICA Clients you plan to deploy, located in the ICAClientDoc directory on the Components CD-ROM.

Features Included in Feature Release 1

MetaFrame XP 1.0, Feature Release 1 includes the following new features and enhancements.

**Important** New features in Feature Release 1 are not available when a server farm operates in mixed mode for interoperability with MetaFrame 1.8

Automatic reconnection to ICA sessions. With the auto client reconnect feature, the ICA Win32 Client automatically reconnects to a session when it detects a dropped connection (when network issues outside of MetaFrame XP occur). Users can continue to work without reconnecting manually, reentering credentials, and restarting applications. The ICA Java Client in embedded mode supports basic automatic reconnection without credential caching (users must reenter their credentials to reconnect).

For more information, see “Reconnecting ICA Sessions Automatically” on page 276.
**Content Publishing.** This feature lets you publish document files, media files, Web URLs, and any other type of file from any network location. Icons for published content appear in Program Neighborhood, on the desktop, and in the Web Interface. Users can double-click published content icons to access content in the same way they access published applications.

For more information, see “Publishing Content” on page 258.

**Connection control.** This feature lets you set a limit on the number of connections that each user can have simultaneously in the server farm. You can also limit the number of concurrent connections to specified published applications, and you can prevent users from launching more than one instance of the same published application.

For more information, see “Controlling User Connections” on page 266.

**Prioritizing CPU access by applications.** You can use the CPU prioritization feature to assign each published application in the server farm a priority level for CPU access. This feature can be used to ensure that CPU-intensive applications in the server farm do not degrade performance of other applications. You can give a higher CPU priority to mission-critical published applications and a lower CPU priority to less-important applications.

For more information, see “Setting CPU Priority Levels for Applications” on page 261.

**Universal Printing**  A universal printer driver is included with Feature Release 1. This driver can be installed in the server farm and used as the driver for all printers that users running the ICA Win32 Client print to in the server farm. The universal driver eliminates the need to install many separate printer drivers for diverse printing environments.

For more information, see “Using MetaFrame XP Universal Printing” on page 306.

**NDS Support.** Support for Novell Directory Services allows users in Novell network environments to log on using their NDS credentials to access applications and content published in MetaFrame XP server farms.

For more information, see “Using the Management Console for MetaFrame XP” on page 177.

**SSL support for ICA.** This feature enables use of the Secure Sockets Layer (SSL) protocol to secure communication between ICA Clients that support SSL and MetaFrame XP servers. SSL provides server authentication, encryption of the data stream, and message integrity checks. After configuring the Citrix SSL Relay, you can specify the use of SSL when you publish applications.
For information about configuring clients for SSL, see the *ICA Win32 Client Administrator’s Guide*. For information about server configuration of the Citrix SSL Relay, see “Setting up Citrix SSL Relay” on page 162.

**Web-based administration.** You can install the Citrix Web Console on MetaFrame XP servers that have Internet Information Services 5.0 or later installed. You can then monitor MetaFrame XP server farms from any workstation with a supported Web browser. The Citrix Web Console lets you view information about the server farm, published applications, servers, and active sessions, and lets you reset, disconnect, and shadow ICA sessions and send messages to users.

For more information, see “Citrix Web Console” on page 181 and the online help available from the console.

**MetaFrame XPe components.** Feature Release 1 includes enhancements to Resource Manager, Installation Manager, and Network Manager, which are part of MetaFrame XPe.

**ICA session monitoring.** New performance counters for ICA data let you use the Windows Performance Monitor to monitor ICA communication, including bandwidth and compression for sessions, servers, and individual virtual channels, and latency in ICA sessions. Performance monitoring can provide valuable information about utilization of network bandwidth and help determine if a bottleneck exists.

For more information, see “Monitoring Performance of Sessions and Servers” on page 288.

**Management Console for MetaFrame XP improvements.** More detailed information about servers and licensing now appears in the Management Console. For example, the Licensing Summary tab now shows the name of feature releases that you install, the number of servers set up to use feature releases, and the feature release licenses that are installed in the server farm.

For more information, see “Viewing Feature Release License Information” on page 156. For information about all new options in the Management Console for MetaFrame XP, see the console’s online help.

**Extended Parameter Passing.** With Feature Release 1, you can associate a file type on a client device with an application published on a MetaFrame XP server. When a user double-clicks a local file, the ICA Client passes the file path as a parameter to the MetaFrame XP server. The server retrieves the file and opens it with the associated application in an ICA session. For more information, see “Associating Published Applications with File Types” on page 250.

Version 6.20 of the ICA Win32 Client was included with Feature Release 1 for MetaFrame XP. The following are brief descriptions of new features in that release.
For more information about features and improvements included in the ICA Clients that shipped with Feature Release 1, see the ICA Client Administrator’s Guides, which are in the ICAClientDoc folder on the MetaFrame XP Components CD-ROM.

**Citrix Program Neighborhood Agent.** Use the Citrix Program Neighborhood Agent to deliver published applications directly to users’ desktops, so users can access links to published applications with or without a Web browser. With the Program Neighborhood Agent, links to published applications appear in the Start menu, on the Windows desktop, or in the Windows System Tray. Remote applications are integrated into the desktop and appear to the user as local applications. You must use the Web Interface for MetaFrame XP to use the Program Neighborhood Agent.

**SSL support for ICA.** Citrix SSL Relay secures data communications using the Secure Sockets Layer (SSL) protocol. SSL provides server authentication, encryption of the data stream, and message integrity checks. You can now use Citrix SSL Relay to secure communications between an SSL-enabled ICA Win32 Client and a MetaFrame XP server.

**Windows Installer Packages for ICA Win32 Clients.** The ICA Win32 full Program Neighborhood Client and the Program Neighborhood Agent are now available in Microsoft Windows installer packages (.msi files), which you can deploy with Windows Installer technology.

### Features in MetaFrame XP

The following are new or significantly enhanced features in MetaFrame XP 1.0. For information about MetaFrame XP feature releases, see “MetaFrame XP Feature Releases” on page 26.

**Enhanced scalability.** Large enterprise-wide server farms can be easily installed, managed, and expanded as business requirements demand. The IMA foundation supports complex network configurations, including multiple network segments and firewalls. The loss of any single server does not impact the functioning of a server farm.

**Integrated security.** MetaFrame XP server farms are resistant to security threats that could damage the farm or lead to theft of information and denial of service. SecureICA high encryption is integrated into the base product, so data on the network is protected with 128-bit encryption.

**Integration with the Web Interface for MetaFrame XP.** A Web Interface is included with MetaFrame XP and installed by default on MetaFrame XP servers. The Web Interface provides Program Neighborhood functionality for Web browser clients to access MetaFrame XP servers.
Licensing. IMA provides enhancements that make MetaFrame XP license administration easier. Improvements include single-point license installation and activation, and farm-wide connection license pooling among IMA-based MetaFrame XP servers.

SNMP support. MetaFrame XP includes support for administrative event notification and basic management control of MetaFrame XP servers through third-party management products (Tivoli and OpenView) using Simple Network Management Protocol (SNMP).

Printer management. MetaFrame XP provides robust control over printer devices. Configurable options include client printer mapping, automatic and on-demand replication of printer drivers, and printer resource assignment.

Application migration. Applications that are published on MetaFrame 1.8 servers can be migrated transparently to MetaFrame XP servers with all configuration data, including user authorizations and connection settings, intact.

Interoperability. MetaFrame XP server farms can coexist with MetaFrame 1.8 servers and MetaFrame for UNIX Operating Systems 1.x servers.

Installation. MetaFrame XP Setup supports attended and unattended installation. You can use Setup to install any or all of the components of your MetaFrame XP family level, including MetaFrame XP Server software, ICA Clients, and the Management Console for MetaFrame XP.

Shadowing options. Administrators can enable shadowing notification or disable shadowing completely during MetaFrame XP installation. A shadowing indicator appears on the ICA Client desktop during shadowing and allows users to cancel shadowing easily with the mouse or a keyboard shortcut.

Display options. MetaFrame XP provides greater display capabilities while efficiently utilizing existing bandwidth. ICA Client users and administrators can select more colors and larger screen sizes than were supported by earlier MetaFrame XP servers.
CHAPTER 3

Planning for MetaFrame XP Deployment

This chapter includes background information about decisions you need to make before you deploy MetaFrame XP. Be sure to read this chapter before you install MetaFrame XP on your servers.

System Requirements

This section describes minimum configurations and recommendations for installing MetaFrame XP on servers. For information about system requirements for ICA Client devices, see the ICA Client Administrator’s Guide for each client platform.

System Software Requirements

You can install MetaFrame XP with Feature Release 3 on servers running the following Microsoft operating systems:


Important You must install the Terminal Services component before you install MetaFrame XP. Terminal Services is not installed with Windows by default; you can install it with Add/Remove Programs in Control Panel. Install Terminal Services in Application Server mode.
Running MetaFrame XP on Windows Server 2003

MetaFrame XP on Windows Server 2003 includes the following changes in functionality.

The ICA Client Creator utility is not supported. If you want to create installation floppy diskettes for supported ICA Clients, you must manually create them.

Virtual “Scripts” directory is not created when IIS is enabled. MetaFrame XP Setup installs two .Dll files — wpnbr.dll and clm.dll — in a virtual directory called “Scripts.” These files are required if you are using the Web Interface for MetaFrame XP for port sharing (wpnbr.dll) or if you are using iLicensing (clm.dll).

If MetaFrame XP Setup does not detect a virtual directory called “Scripts,” Setup creates a physical directory under %SystemRoot%\inetpub\Scripts.

Remote users can connect to MetaFrame XP servers over TCP/IP only. Terminal Services in Windows Server does not support remote connections over IPX/SPX, NetBIOS, and asynchronous transports.

Microsoft Java Virtual Machine (JVM) is not installed. If you install the Web Interface for MetaFrame XP and the setup program does not detect the Microsoft JVM, you are prompted to install it. A redistributable copy of the Microsoft JVM is included in the MetaFrame XP media.

“Restrict each user to one session” feature is enabled by default. When this setting is enabled, the server disconnects an active session and reconnects the new connection request from the same user to the disconnected session. Enabling this feature conserves resources and simplifies reconnecting to disconnected sessions.

You can disable this setting in the Server Settings node of Terminal Services Configuration.

Users must be members of the Remote Desktop Users group to connect through Terminal Services. By default, there are no users in the Remote Desktop Users group, so users are blocked from connecting remotely. MetaFrame XP Setup allows you to add the members of the local Users group to the Remote Desktop Users group. If you skip the step of adding users to the Remote Desktop Users group, you must add users to this group after Setup completes.

Requirements for the Web Interface for MetaFrame XP

To install the Web Interface on a MetaFrame XP server, Microsoft Internet Information Services (IIS) Version 5.0 or higher and the Microsoft Java Virtual Machine (JVM) must be installed before you install MetaFrame XP.
Naming Servers and Server Farms

You assign a name to your MetaFrame XP server farm when you install MetaFrame XP on the first server in the farm. The server farm name can contain 32 or fewer characters. Server farm names are case-sensitive.

For a MetaFrame XP server farm to operate in mixed mode with an existing MetaFrame 1.8 server farm, you must assign the name of the MetaFrame 1.8 server farm when you create the MetaFrame XP server farm.

MetaFrame server names must be unique, whether the servers are in MetaFrame XP server farms or in mixed-mode MetaFrame XP and MetaFrame 1.8 server farms. If necessary, change the name of a server before installing MetaFrame XP.

**Important**  MetaFrame XP supports server names that contain extended characters only if your network’s DNS server supports names with extended characters.

System Hardware Requirements

The following requirements are based on the requirements of the operating systems on which you run MetaFrame XP.

**Windows 2000 Server and Advanced Server.**  Microsoft recommends a 166MHz or faster Pentium-compatible processor, 256MB of RAM, and a 2GB hard disk with at least 1GB of free space.

**Windows 2000 Datacenter Server.**  Microsoft recommends an eight-way or greater array of Pentium III Xeon processors, 256MB of RAM, and a 2GB hard disk with at least 1GB of free space.

**Windows Server 2003, Standard Edition.**  Microsoft recommends a 550MHz or faster Pentium-compatible processor, 256MB of RAM, and a 2GB hard disk with at least 1.5GB of free space.

**Windows Server 2003, Enterprise Edition.**  Microsoft recommends a 733MHz or faster Pentium-compatible processor, 256MB of RAM, and a 2GB hard disk with at least 1.5GB of free space.

**Windows Server 2003, Datacenter Edition.**  Microsoft recommends a 733MHz or faster Pentium-compatible processor, 1GB of RAM, and a 2GB hard disk with at least 1.5GB of free space.
**Important** Microsoft recommends that you do not install Terminal Services on a Windows server acting as a domain controller. By default, users cannot log on to Terminal Services sessions on a domain controller. You can permit users to log on by setting the “log on locally” right; however, this is not recommended.

**Disk and Memory Requirements**

In addition to the Windows operating system requirements for your server, use the following guidelines for MetaFrame XP:

- 250MB disk space for installing the MetaFrame XPe family level
- 150MB disk space for installing all ICA Client software

**Modems and Multiport Adapters**

In addition to ICA connections over network protocols (see “Configuring Network ICA Connections” on page 125), MetaFrame XP supports asynchronous ICA connections.

When you set up an asynchronous ICA connection on a MetaFrame XP server, client devices with modems can dial up the modem on a MetaFrame XP server. When they connect, the ICA Client and MetaFrame XP server communicate directly, without the overhead of Windows Remote Access Service (RAS) and TCP/IP.

If you want to configure modems for ICA dial up connections and the modems are configured for Windows RAS, remove the modems from the RAS modem pool before you start MetaFrame XP installation.

**Important** You cannot configure a modem or serial port as both a RAS service port and an ICA asynchronous connection port.

For ICA asynchronous connections, Citrix recommends high-speed serial port hardware or intelligent multiport adapters on the server. These devices use the CPU efficiently, freeing CPU resources that can be devoted to running user sessions. If you have a multiport async adapter, install it before starting MetaFrame XP installation.
Management Console for MetaFrame XP Requirements

The Management Console for MetaFrame XP is the centralized management utility you use to administer your MetaFrame XP server farm. It is installed on all MetaFrame XP servers by default. However, using the MetaFrame XP CD, you can install the Management Console on workstations that are not used as MetaFrame XP servers. Computers intended to run the console must meet the following requirements:

**Operating system.** You can install the Management Console on any workstation running Windows NT 4.0, Windows 2000, or Windows XP. You can install the console on your MetaFrame XP servers, but the console does not require that MetaFrame XP be installed on the same computer.

**Sun Java Runtime Environment (JRE).** The Management Console is a Java application and requires the Sun JRE Version 1.4.1. If your system does not have the JRE, Setup installs Version 1.4.1, the version required to run the console. The console does not run on JRE Version 1.3.1. If you have this version of the JRE installed on the target system, Setup still installs Version 1.4.1 and Version 1.3.1 remains installed.

**Disk space.** A minimum of 50MB of disk space is required for installation of the Management Console and the Java Run-Time Environment.

**Memory.** A minimum of 64MB of RAM is needed for running the Management Console (in addition to RAM required for the operating system and other applications).

**Processor.** A Pentium-class or better processor is recommended.

---

**Sizing Systems for MetaFrame XP**

MetaFrame XP supports multiple users on Windows 2000 and Windows Server 2003 servers. A multiuser system requires more system resources than a single-user system. This section provides some system-sizing guidelines that can help you decide on a hardware configuration that will support your users with optimal performance.
Note  More information about system sizing, optimization, configuration, and deployment scenarios is included in Advanced Concepts for MetaFrame XP. This guide is available from the Support area of the Citrix Web site at www.citrix.com/support. Select Product Documentation.

Most companies find that their users can be categorized as typical users or power users.

**Typical user.** Generally uses one or two applications but normally only one at a time. Little actual program data is transferred between the client and server, and the users rarely use Object Linking and Embedding (OLE).

**Power user.** A more sophisticated user who uses three or more applications, often with several active at the same time. Data is often cut and pasted between local and remote applications, and OLE is used heavily.

Power users consume more resources than typical users. A good rule of thumb is that one power user is equivalent to two typical users in processor utilization and RAM requirements.

Tip  The configuration examples in this section are based on numbers of typical users. Adjust the numbers for power users.

**Processor, Bus, and Memory**

The processor and bus architecture are fundamental to MetaFrame XP server performance.

The ISA (AT bus) architecture is low-bandwidth and is not recommended for MetaFrame XP servers. Use a higher-performance bus, such as EISA or PCI, for best performance. These buses support the high sustained data transfer rates that are typical of a MetaFrame XP server.

The memory (RAM) requirement for MetaFrame XP is 16MB plus 4MB for each typical user or 8MB for each power user. In many cases, adding RAM has a larger effect on system performance than upgrading to a faster processor.

In general, processor and RAM requirements for MetaFrame XP scale linearly. You can roughly double the number of users supported on a multiprocessor-capable system by doubling the number of processors and doubling the amount of RAM. By purchasing multiprocessor-capable systems (even if you initially purchase only one processor), you provide for convenient system scaling as your requirements grow.
Note that not all multiprocessor systems scale the same way because of bus differences. The bus architecture in a multiprocessor system is crucial for multiprocessor performance with more than four processors, and vendor-specific drivers are usually required.

**Win16 Application Requirements**

Windows NT and Windows 2000 are Win32 (32-bit) environments. Windows 3.x for DOS is a Win16 (16-bit) environment. Windows NT and Windows 2000 run Win16 applications through a process called WOW (Win16 on Win32), which translates 16-bit applications in enhanced mode. This process causes Win16 applications to consume additional system resources, reducing the number of users per processor by 20% and increasing the RAM required per user by 25%. For this reason, use Win32 applications whenever possible. If you intend to run Win16 applications, adjust your processor and RAM requirements accordingly.

**Hard Disks**

The hard disk subsystem in a server is an important factor in system throughput. Small Computer System Interface (SCSI) disk drives and adapters, especially Fast Narrow SCSI (SCSI-2), Fast Wide SCSI, Wide Ultra SCSI, and Wide Ultra2 SCSI devices, have significantly better throughput than ST-506, Integrated Device Electronics (IDE), or Enhanced Small Device Interface (ESDI) disk drives and adapters.

For the highest disk performance, consider using a SCSI-based Redundant Array of Independent Disks (RAID) controller. RAID controllers automatically place data on multiple disk drives and can increase disk performance and improve data reliability.

Use NTFS for all disk partitions on your MetaFrame XP servers. NTFS allows security configuration, better performance, and more fault tolerance.

**Network Interfaces**

The ICA protocol is highly compressed and causes negligible loading on a network, but because the MetaFrame XP server handles all network requests, a high-performance network interface card (NIC) is recommended.

If a multiport asynchronous communications adapter is installed for supporting serial ICA connections, be sure to use an intelligent (microprocessor-based) adapter to reduce interrupt overhead and increase throughput.
Using Performance Monitoring Tools

Citrix recommends that you use performance monitoring tools to get accurate accounts of system performance and the effects of configuration changes on system throughput. The most important measurements for performance monitoring are the percentage of total processor time, memory pages per second, percentage of network utilization, and hard disk I/O rates.

Resource and network management and monitoring features are included with MetaFrame XPe. Updated documentation for these components of MetaFrame XPe is included in the Docs directory on the MetaFrame XP Server CD.

A good way to estimate how many users a server can support is to measure system performance with two to five users on the system and then scale the results. This method has been found to yield reliable results.

For information about performance-monitoring counters available for monitoring ICA and MetaFrame XP servers, see “Monitoring Performance of Sessions and Servers” on page 288.

Choosing a Database for the Data Store

Before installing MetaFrame XP, you must decide which database to use for your farm’s data store.

MetaFrame XP is compatible with the following database software:

- **Microsoft Access.** Access is a lightweight database that is included with Windows server operating systems. The Access database is created on the first MetaFrame XP server in a new server farm. It is most appropriate for small to mid-sized server farms.

- **Microsoft SQL Server 2000 Database Engine (MSDE).** MSDE is a database engine based on Microsoft SQL Server core technology. The MSDE database is created on the first MetaFrame XP server in a new server farm. It is most appropriate for small to mid-sized server farms and can be administered using standard Microsoft SQL Server tools.

- **Microsoft SQL Server.** SQL Server is a true client/server database that offers robust and scalable support for multiple-server data access. It is suited for use in farms of any size.

- **Oracle.** Oracle is a true client/server database that offers robust and scalable support for multiple-server data access. It is suited for use in farms of any size.

- **IBM DB2.** DB2 is a true client/server database that offers robust and scalable support for multiple-server data access. It is suited for use in farms of any size.
When using Microsoft Access, the database is created when you run MetaFrame XP Setup. When using MSDE, you install MSDE and then create the database when you run MetaFrame XP Setup. The database is stored on the first MetaFrame XP server in the farm.

When using Microsoft SQL Server, Oracle, or IBM DB2, the database is on a server dedicated to running the database product. This dedicated server must be set up prior to creating the server farm because you will need to configure an ODBC connection to it. MetaFrame XP servers must also have the appropriate database client software installed on them.

You should consider many factors before you decide which database product to use for your server farm’s data store, including but not limited to:

- The number of MetaFrame XP servers you currently plan to have in the server farm and whether you plan to expand the number of servers in the farm
- Whether you have a database administrator on staff with the expertise to configure and manage a data store running on SQL Server, Oracle, or DB2
- Whether you foresee the organization expanding, and therefore expanding the number and type of published applications
- Whether the database can sustain an increase in the number of users and connections
- Whether a MetaFrame server has the appropriate hardware configuration to also run an Access or MSDE database or whether you require that the database be located on a server that is not also running MetaFrame XP
- Any database maintenance requirements you may have, such as backup, redundancy, and replication

**Important** Microsoft SQL, Oracle, and IBM DB2 servers require significant expertise to install and maintain. If you do not have expertise with these products, attempting to use them in a production environment is not recommended. See the documentation included with your database product for important details such as performance tuning and database backup procedures.

For information about supported database and ODBC driver versions, see “Data Store Database Requirements” on page 55.

**CAUTION** Do not install MetaFrame XP on the Microsoft SQL, Oracle, or IBM DB2 database server. See your database product’s documentation for specific hardware requirements for the database server.
System Sizing for the Data Store Database

The choice of which database to use for your MetaFrame XP server farm’s data store depends greatly on your implementation and environment.

Use the chart below as a guideline to determine which scenario most closely matches your environment. If your environment doesn’t fit neatly into the categories listed, choose the category that has the most in common with your environment.

<table>
<thead>
<tr>
<th></th>
<th>Small</th>
<th>Medium</th>
<th>Large</th>
<th>Enterprise</th>
</tr>
</thead>
<tbody>
<tr>
<td>Servers</td>
<td>1-50</td>
<td>25-100</td>
<td>50-100</td>
<td>100 or more</td>
</tr>
<tr>
<td>Named Users</td>
<td>&lt; 150</td>
<td>&lt; 3000</td>
<td>&lt; 5000</td>
<td>&gt; 3000</td>
</tr>
<tr>
<td>Applications</td>
<td>&lt; 100</td>
<td>&lt; 100</td>
<td>&lt; 500</td>
<td>&lt; 2000</td>
</tr>
</tbody>
</table>

The following are general recommendations for the server farm’s data store database:

- Microsoft Access and MSDE are suitable for all small and many medium-sized environments
- Microsoft SQL, Oracle, and IBM DB2 are suitable for any size environment and are especially recommended for all large and enterprise environments

Note: If you plan to use mixed mode to support MetaFrame 1.8 servers, do not include the MetaFrame 1.8 servers in your system sizing calculations.

Suggested Hardware Configurations for the Data Store

This section outlines suggested hardware configurations resulting from extensive testing in the Citrix eLab. All tests used Microsoft SQL Server 2000 in the default configuration without replication for the server farm’s data store.

Increasing the CPU power and speed of the database server can improve the response time to queries made to the MetaFrame XP data store. Increase the processing power of the data store database server to achieve improved results in the following areas:

- Starting the Citrix IMA Service on multiple servers simultaneously
- Adding a license to the farm
- Adding a server to the farm
- Removing a server from the farm
The response time of other events occurring in the server farm — such as starting the IMA service on a single server, recreating the local host cache, or replicating printer drivers to all servers in the server farm — is affected more by the size of the farm than by the response time of the data store.

Extensive testing in the Citrix eLab shows that adding processors to the server hosting the data store can dramatically improve response time when multiple simultaneous queries are being executed. If the environment includes large numbers of servers coming online simultaneously and at frequent intervals, the additional processors can service requests faster.

However, with serial events such as joining servers to a MetaFrame XP server farm or removing servers from a server farm, adding processors can result in lower performance gains. To improve the processing time for serial events, increase the processor speed of the hardware hosting the data store.

The actual performance of a server farm’s data store can vary depending upon which database engine is used and the level of performance tuning that can be achieved. Depending on the characteristics of a MetaFrame XP server farm, the CPU speed and quantity can vary widely.

In the chart below, five sample server farm configurations are displayed and referred to as scenarios A through E. Each scenario lists measurements of various metrics in the server farm.

The second chart shows which hardware configurations are suggested in a MetaFrame XP farm similar to the corresponding scenario.

<table>
<thead>
<tr>
<th>Scenario</th>
<th>A</th>
<th>B</th>
<th>C</th>
<th>D</th>
<th>E</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of servers in farm</td>
<td>80</td>
<td>160</td>
<td>250</td>
<td>350</td>
<td>500</td>
</tr>
<tr>
<td>Number of applications published to all servers</td>
<td>50</td>
<td>50</td>
<td>50</td>
<td>50</td>
<td>50</td>
</tr>
<tr>
<td>Number of user policies</td>
<td>25</td>
<td>25</td>
<td>25</td>
<td>25</td>
<td>25</td>
</tr>
<tr>
<td>License packs</td>
<td>11</td>
<td>19</td>
<td>28</td>
<td>38</td>
<td>53</td>
</tr>
<tr>
<td>Printers per server</td>
<td>5</td>
<td>5</td>
<td>5</td>
<td>5</td>
<td>5</td>
</tr>
<tr>
<td>Printer drivers installed per server</td>
<td>25</td>
<td>25</td>
<td>25</td>
<td>25</td>
<td>25</td>
</tr>
<tr>
<td>Network print servers with printers</td>
<td>5</td>
<td>5</td>
<td>5</td>
<td>5</td>
<td>5</td>
</tr>
<tr>
<td>Number of Load Manager load evaluators</td>
<td>10</td>
<td>10</td>
<td>10</td>
<td>10</td>
<td>10</td>
</tr>
<tr>
<td>Number of Resource Manager applications</td>
<td>10</td>
<td>10</td>
<td>10</td>
<td>10</td>
<td>10</td>
</tr>
<tr>
<td>Number of Installation Manager groups</td>
<td>5</td>
<td>5</td>
<td>5</td>
<td>5</td>
<td>5</td>
</tr>
<tr>
<td>Number of Installation Manager packages</td>
<td>5</td>
<td>5</td>
<td>5</td>
<td>5</td>
<td>5</td>
</tr>
</tbody>
</table>
Connecting to the Data Store

After you decide which database to use for the data store, decide whether MetaFrame XP servers will connect directly to it or indirectly through another MetaFrame XP server.

To make a direct connection to the data store, a MetaFrame XP server must have the appropriate ODBC drivers installed and configured properly. The MetaFrame XP server then connects directly to the server on which the database is running.

For indirect access, a MetaFrame XP server connects to an intermediary MetaFrame XP server. The intermediary server connects to the data store directly. Using indirect connectivity with a SQL Server database eliminates the need to install and configure the ODBC drivers on every MetaFrame XP server. If you are using a SQL Server database for the data store, you can use a combination of direct and indirect access methods for the servers in the farm.

Indirect access is not recommended for mission-critical server farms because the intermediary server is a single point of failure.
Note Although it is possible to configure multiple MetaFrame XP servers to connect directly to a single MSDE database, Citrix does not recommend this configuration because it is not supported by MSDE. MSDE allows only five connections per installed instance of MSDE. If more than five MetaFrame XP servers attempt to access the MSDE database at the same time, they cannot connect. Citrix recommends that you configure an MSDE database for indirect access.

By default, indirect access uses TCP port 2512 for communication among the MetaFrame XP servers. If the MetaFrame XP servers are in different subnets, be sure this port is not blocked by any firewalls. If this port number is not convenient, it can be changed.

Important If you recreate the server farm’s data store database, a MetaFrame XP administrator account with full administration rights is created using the local administrator account credentials. Be sure to create a new MetaFrame XP administrator with full administration rights in the Management Console for MetaFrame XP. Doing so replaces the default MetaFrame XP administrator account that uses the local administrator credentials.

Be sure to back up any database before you attempt to recreate it.

Data Store Database Requirements

You can use the Microsoft Access or MSDE database engines or a Microsoft SQL Server, Oracle, or IBM DB2 database for the server farm’s data store. The supported ODBC drivers and database versions are listed below.

Microsoft Access

Choosing **Use a local database on this server** and selecting the Access Database entry from the list of possible databases during MetaFrame XP Setup creates a Microsoft Access database on the MetaFrame XP server. This database acts as the server farm’s data store.

The Microsoft Access database engine and ODBC drivers are default components of Windows Servers. The ODBC connection to Access uses the Microsoft Jet Engine. To use the database engine, you do not have to install any drivers or perform any database configuration prior to MetaFrame XP installation.

Minimum Requirements

The MetaFrame XP server that hosts the Access database should meet the following minimum requirements:
Approximately 50MB of disk space for every 100 servers and 25 applications in the farm

32MB of additional RAM if the MetaFrame XP server will also host connections

**Authenticating to the Access Database**

If you decide to create a local Access database on the MetaFrame XP server, MetaFrame XP Setup creates a database called “mf20.mdb.” The user name and password for this database file are blank.

You can use the **Dsmaint** command (dsmaint config /pwd:newpassword) to change the password on the database. The Citrix IMA Service can be running when you use the command. Keep the new password in a secure place so you can access it if you want to migrate to another database.

**Important** Be sure to back up the Access database using the **Dsmaint** command (dsmaint backup) before changing the password used to access the database.

For more information about MetaFrame XP commands, see “MetaFrame XP Commands” on page 311.

**Microsoft SQL Server 2000 Desktop Engine (MSDE)**

You can use SQL Server Desktop (MSDE) for your server farm’s data store. To use MSDE, you must install it on the MetaFrame XP server before you run MetaFrame XP Setup.

You can install MSDE on the MetaFrame XP server using one of the following methods:

- Run the SetupMsdeForMetaFrame.cmd batch file. Use this method if you do not have an instance of MSDE already installed on the MetaFrame XP server and you want to use the default MSDE instance name and password values.
- Launch MSDE Setup from a command prompt. Use this method if you cannot use the default MSDE instance name and password. You must install MetaFrame XP Server using a manual method if you specify an instance name for MSDE different from the default.

- **To install MSDE 2000 with Service Pack 3 using default options**

If you do not have an instance of MSDE already installed on the MetaFrame XP server and you are not using SQL authentication, you can run SetupMsdeForMetaFrame.cmd, located on the MetaFrame XP Server CD in the directory Support\MSDE.
Running the SetupMsdeForMetaFrame.cmd batch file installs MSDE 2000 with Service Pack 3 using the default instance name “CITRIX_METAFRAME” and sets the MSDE administrator (“SA”) password to “CITRIX.”

After you install MSDE, choose Use a local database on this server and select the SQL Server Desktop (MSDE) Database entry from the list of possible databases during MetaFrame XP Setup to use MSDE for the server farm’s data store.

**Note**  The MSDE SA password is required to be set; however, SQL authentication is not enabled by default when you install MSDE using SetupMsdeForMetaFrame.cmd. Because SQL authentication is not enabled, the SA password is not used. Setting the password to “CITRIX” is not a security risk unless you are using SQL authentication.

If you want to specify a different SA password for an instance of MSDE, install MSDE using the installation method below.

If you need to specify an instance name and SA password, follow the procedure below to install MSDE at a command prompt using custom options.

**Important**  If you install MSDE and specify an instance name different from the default “CITRIX_METAFRAME,” you must install MetaFrame XP Server using a manual installation method so that you can set the MetaFrame XP Server Setup property CTX_MF_MSDE_INSTANCE_NAME to the new instance name. See “Customizing MetaFrame Setup” on page 367 for more information about setting MetaFrame XP Server Setup properties.

### To install MSDE 2000 with Service Pack 3 using custom options

1. At a command prompt, change to the Support\MSDE\MSDE directory on the MetaFrame XP Server CD. For example, if your CD drive is E, type:
   
   ```
   E:
   cd \Support\MSDE\MSDE
   ```

2. Change to installation mode by typing:
   
   ```
   change user /INSTALL
   ```

3. Launch the MSDE installer, specifying the instance name and SA password. For example, type:
   
   ```
   setup.exe INSTANCENAME=<name> SAPWD=<password>
   ```

**Important**  Citrix strongly recommends that you use the version of MSDE (MSDE 2000 with Service Pack 3) included on the MetaFrame XP Server CD.
**Important** If you intend to use MSDE to host your server farm’s data store, do not use double-byte characters in the name of the server on which the MSDE database will be stored.

**Minimum Requirements**

The MetaFrame XP server that hosts the MSDE database should meet the following minimum requirements:

- Approximately 50MB of disk space for every 100 servers and 25 applications in the farm
- 32MB of additional RAM if the MetaFrame XP server will also host connections
- 70MB of disk space for the MSDE database

**Authenticating to the MSDE Database**

Windows NT authentication is supported for the MSDE database. For security reasons, Microsoft SQL Server authentication is not supported.

**Migrating to MSDE**

You can migrate only a data store using Microsoft Access to MSDE. Run the `MigrateToMsde` utility, located in the `Support\MSDE` directory on the MetaFrame XP Server CD, to migrate from Access to MSDE.

For more information about the `MigrateToMsde` utility, see “MetaFrame XP Commands” on page 311.

**Microsoft SQL Server**

MetaFrame XP supports the following versions of Microsoft SQL Server for the server farm’s data store.

- **Microsoft SQL Server 7.** Microsoft SQL Server 7 with Service Pack 2 or Service Pack 3 is supported on Windows NT 4.0 Server and Windows 2000 Server family.
  
  Version 3.70.08.20 or greater of the Microsoft SQL ODBC driver must be installed on each MetaFrame XP server that will directly access the SQL server.
  
  - On Windows 2000 servers, the necessary drivers are installed with the operating system.
  
  - On Windows NT 4.0 Server, install Microsoft Data Access Components (MDAC) Version 2.6 with Service Pack 1, which can be downloaded for free from Microsoft’s download site. Do not use MDAC 2.6 without Service Pack 1.
Important On Windows NT 4.0, TSE systems, stop the Terminal Services Licensing Service before installing MDAC. After installing MDAC, clear the event log, then restart the server before installing MetaFrame XP.


On Windows NT 4.0 Server, Windows NT Service Pack 5 (SP 5) or later must be installed for all SQL Server 2000 editions.

The following configurations have been verified by Citrix testing:

- MDAC 2.5, Windows 2000 Server, SQL Server 2000
- MDAC 2.51, Windows 2000 Server with SP1 or SP2, SQL Server 2000
- MDAC 2.51, Windows 2000 Server with SP1 or SP2, SQL Server 2000 with SP1
- MDAC 2.6 SP1, Windows 2000 Server with SP1 or SP2, SQL Server 2000 with SP1

Important MDAC 2.6 without SP1 is not supported because of an issue with the driver.

Minimum Requirements

The practices outlined in this section are suggested practices for using Microsoft SQL Server as the data store. Be sure to read the Microsoft SQL Server documentation before you install and configure Microsoft SQL Server.

The following minimum requirements can apply to MetaFrame XP implementations that use SQL Server as the farm’s data store:

- There should be approximately 100MB of disk space for every 250 servers and 50 published applications in the farm. The required disk space increases if a large number of published applications are in the farm.
- Set the “temp” database to automatically grow on a partition with at least 1GB of free disk space. 4GB is recommended if the MetaFrame XP server farm is large and includes multiple print drivers.

Note Make sure that enough disk space exists on the server to support growth of both the “temp” database and the data store database.
Authenticating to the Microsoft SQL Server Database

Consider the following issues when planning authentication to the SQL Server database:

- Microsoft SQL Server supports Windows NT and Microsoft SQL Server authentication. Consult the Microsoft SQL Server documentation for configuring Windows NT authentication support. For high-security environments, Citrix recommends using Windows NT authentication only.
- The user account used for connecting to the data store must have database owner (“db_owner”) rights to the database.
- When you are done installing the database with database owner rights, set the user permissions to read/write only. Doing this increases the security of the database.

**Important** If you change the rights from database owner to read/write, be sure to change the rights back to database owner before you attempt to install MetaFrame XP service packs or feature releases. Installation of MetaFrame XP service packs or feature releases can fail if the user account you use to authenticate to the data store during Setup does not have database owner rights.

Migrating to SQL Server

Migration of a MetaFrame XP server farm data store to Microsoft SQL Server is supported for the database versions listed in the following table. For information about data store migration, see the **Dsmaint** command on page 343.

<table>
<thead>
<tr>
<th>Original platform</th>
<th>Target platform</th>
</tr>
</thead>
<tbody>
<tr>
<td>Microsoft Access</td>
<td>SQL Server 7 with SP3</td>
</tr>
<tr>
<td>Microsoft Access</td>
<td>SQL Server 2000</td>
</tr>
<tr>
<td>Microsoft Access</td>
<td>SQL Server 2000 with SP1</td>
</tr>
<tr>
<td>MSDE</td>
<td>SQL Server 2000</td>
</tr>
<tr>
<td>Oracle 8.1.6</td>
<td>SQL Server 2000 with SP1</td>
</tr>
<tr>
<td>Oracle 8.1.7</td>
<td>SQL Server 2000 with SP1</td>
</tr>
<tr>
<td>Oracle9i</td>
<td>SQL Server 2000 with SP1</td>
</tr>
<tr>
<td>IBM DB2 with FixPak 5</td>
<td>SQL Server 2000 with SP1</td>
</tr>
</tbody>
</table>
Oracle

MetaFrame XP supports the following Oracle databases for the server farm’s data store:

- Oracle9i, Enterprise Edition Database Release 1
- Oracle8i, Version 8.1.6 and 8.1.7
- Oracle 8, Version 8.0.6
- Oracle 7, Version 7.3.4

If you are using Oracle 8, install the Oracle Net8 client Version 8.1.5.5 or later and ODBC drivers provided by Oracle on each MetaFrame XP server that will directly access the database server. The MetaFrame XP farm’s data store is stored as an object (schema) assigned to a user. You do not need a separate database for each data store.

During install, you can either run the Net8 Easy Config, or cancel the installation at that point and copy the Tnsnames.ora and Sqlnet.ora files from the Oracle server to %oracle home directory%\network\admin on each MetaFrame XP server.

**Important** Restart the system after you install the Oracle client and before you install MetaFrame XP.

In some cases you will need to configure the DNS entry within the Oracle Net8 Assistant. To do this, click **Profile** and then select the **Oracle Names** tab. Enter the DNS suffix that the network is using. You can use the command IPCONFIG /ALL to gather the DNS suffix that must be used.

If you do not restart the server after you install the Oracle client, or if the client requires the DNS suffix to be specified, MetaFrame XP Setup reports the following error: “The procedure entry point OCIUnicodeToCharSet could not be located in the dynamic link library OCI.dll.”

If you are using Oracle9i, install the Oracle9i Administrator client to obtain the Oracle ODBC driver Version 9.0.1.0.1. The Oracle9i Run-time client does not have ODBC driver support, which is required on each MetaFrame XP server that will directly access the database server.

**Minimum Requirements**

The practices outlined below are suggested practices for using an Oracle database for the server farm’s data store. Be sure to read the Oracle documentation before you install and configure Oracle databases.
The following minimum requirements can apply to MetaFrame XP implementations that use Oracle as the farm’s data store. Guidelines given here apply to Oracle7, Oracle8, and Oracle8i, except as noted otherwise.

- There should be approximately 100MB of disk space for every 250 servers and 50 published applications in the farm. The required disk space increases if a large number of published applications are in the farm.

- The Oracle Client (Version 8.1.55 or later) must be installed on the MetaFrame XP server before you install MetaFrame XP. The 8.1.5 client is not supported with MetaFrame XP.

### Authenticating to the Oracle Database

Consider the following issues when planning authentication to the Oracle database:

- Oracle for Solaris supports Oracle authentication only; it does not support Windows NT authentication.

- Oracle for Windows NT supports both Windows NT and Oracle authentication. Consult the Oracle documentation for information about configuring Windows NT authentication.

- The Oracle user account must be the same for every server in the farm because all servers share a common schema.

- If you are using one database to hold information for multiple MetaFrame XP farms, each farm represented in the database must have a different user account because the data store information is stored in the Oracle user account’s schema.

- The account used to connect to the data store database must have the following Oracle permissions:
  - Connect
  - Resource
  - Unlimited Tablespace (optional)
## Migrating to Oracle

Migration of a MetaFrame XP server farm data store to an Oracle database is supported for the database versions listed in the following table. For information about data store migration, see the `Dsmaint` command on page 343.

<table>
<thead>
<tr>
<th>Original platform</th>
<th>Target platform</th>
</tr>
</thead>
<tbody>
<tr>
<td>Microsoft Access</td>
<td>Oracle 7</td>
</tr>
<tr>
<td>Microsoft Access</td>
<td>Oracle 8</td>
</tr>
<tr>
<td>Microsoft Access</td>
<td>Oracle 8.1.6</td>
</tr>
<tr>
<td>Microsoft Access</td>
<td>Oracle 8.1.7</td>
</tr>
<tr>
<td>Microsoft Access</td>
<td>Oracle9i</td>
</tr>
<tr>
<td>MSDE</td>
<td>All Supported Versions of Oracle</td>
</tr>
<tr>
<td>Microsoft SQL Server (SQL 7 with SP2 or SP3 or SQL 2000 with SP1)</td>
<td>Oracle 7</td>
</tr>
<tr>
<td>Microsoft SQL Server (SQL 7 with SP2 or SP3 or SQL 2000 with SP1)</td>
<td>Oracle 8</td>
</tr>
<tr>
<td>Microsoft SQL Server (SQL 7 with SP2 or SP3 or SQL 2000 with SP1)</td>
<td>Oracle 8.1.6</td>
</tr>
<tr>
<td>Microsoft SQL Server (SQL 7 with SP2 or SP3 or SQL 2000 with SP1)</td>
<td>Oracle 8.1.7</td>
</tr>
<tr>
<td>Microsoft SQL Server (SQL 7 with SP2 or SP3 or SQL 2000 with SP1)</td>
<td>Oracle9i</td>
</tr>
<tr>
<td>IBM DB2 with FixPak 5</td>
<td>Oracle 7</td>
</tr>
<tr>
<td>IBM DB2 with FixPak 5</td>
<td>Oracle 8</td>
</tr>
<tr>
<td>IBM DB2 with FixPak 5</td>
<td>Oracle 8.1.6</td>
</tr>
<tr>
<td>IBM DB2 with FixPak 5</td>
<td>Oracle 8.1.7</td>
</tr>
<tr>
<td>IBM DB2 with FixPak 5</td>
<td>Oracle9i</td>
</tr>
</tbody>
</table>
IBM DB2

MetaFrame XP supports IBM DB2 Universal Database Enterprise Edition Version 7.2 for Windows 2000 with FixPak 5 for the server farm’s data store.

**Important** MetaFrame XP uses the data type of binary large object (BLOB) to store information in an IBM DB2 database. IBM DB2 does not support the use of BLOB data types in an updateable replication scenario. Therefore, if your server farm needs to have updateable replicas, use Microsoft SQL Server or Oracle for the farm’s data store instead of IBM DB2.

Install the IBM DB2 Run-Time Client and apply FixPak 5 on each MetaFrame XP server that will directly access the database server. If you have multiple MetaFrame XP farms, create a separate database/tablesace for each farm’s data store.

**Important** Restart the system after you install the IBM DB2 Run-Time client and FixPak5 and before you install MetaFrame XP. You may also need to restart after you install the Run-Time client and before you install FixPak 5. See the DB2 documentation for more information.

**Minimum Requirements**

The practices outlined below are suggested practices for using an IBM DB2 database for the server farm’s data store. Be sure to read the DB2 documentation before you install and configure DB2 databases.

The following minimum requirements can apply to MetaFrame XP implementations that use DB2 as the farm’s data store.

- There should be approximately 100MB of disk space for every 250 servers and 50 published applications in the farm. The required disk space increases if a large number of published applications are in the farm.
- If you create a data source name (DSN) for use with an unattended installation of IBM DB2, Citrix recommends that you create the DSN using the Microsoft ODBC Data Source Administration screen. Doing so ensures that the DSN is populated according to MetaFrame XP requirements for proper connectivity to the DB2 database or tablespace.
- Give the DB2 user account that is used for the MetaFrame XP farm the following permissions:
  - Connect database
  - Create tables
• Register functions to execute to database manager’s process

• Create schemas implicitly

  System administrator (DB2Admin) account permissions are not needed for data store access.

• Configure the following settings to optimize database performance:

  • Increase the value of the Application Control Heap Size (appl_ctl_heap_sz) setting from the default of 128 4KB pages (.5MB) to 512 (2MB). This parameter represents the maximum amount of shared memory available to each application instance running on the node.

  • Increase the value of the Buffer Pool Size (buffpage) setting from the default of 250 4KB pages (1MB) to 75-100% of the size of the database for best performance. This parameter represents the buffer memory the database uses for processing requests.

  • Increase the value of the Application Heap Size (applheapsz) setting from the default of 128 4KB pages (.5MB) to at least 256. This parameter represents the amount of memory available to the database manager for each agent.

Migrating to IBM DB2

Migration of a MetaFrame XP server farm data store to an IBM DB2 database is supported for the database versions listed in the following table. For information about data store migration, see the **Dsmaint** command on page 343.

<table>
<thead>
<tr>
<th>Original platform</th>
<th>Target platform</th>
</tr>
</thead>
<tbody>
<tr>
<td>Microsoft Access</td>
<td>IBM DB2 with FixPak 5</td>
</tr>
<tr>
<td>MSDE</td>
<td>IBM DB2 with FixPak 5</td>
</tr>
<tr>
<td>Microsoft SQL Server 2000 with SP1</td>
<td>IBM DB2 with FixPak 5</td>
</tr>
<tr>
<td>Oracle 7</td>
<td>IBM DB2 with FixPak 5</td>
</tr>
<tr>
<td>Oracle 8</td>
<td>IBM DB2 with FixPak 5</td>
</tr>
<tr>
<td>Oracle 8.1.6</td>
<td>IBM DB2 with FixPak 5</td>
</tr>
<tr>
<td>Oracle 8.1.7</td>
<td>IBM DB2 with FixPak 5</td>
</tr>
<tr>
<td>Oracle9i</td>
<td>IBM DB2 with FixPak 5</td>
</tr>
</tbody>
</table>
The migration of an existing MetaFrame XP server farm data store to IBM DB2 is completed as a single transaction for roll-back purposes. Before migrating the database to DB2, verify that enough log space exists on the target DB2 server to support the migration. If the DB2 server runs out of log space, the migration will fail and roll back.

Network Configuration and Account Authority Issues

Before you implement your MetaFrame XP installation, you must consider issues related to network configuration and the management of user accounts. This section discusses recommended practices for:

- Windows NT (non-Active Directory) and Active Directory domains and groups
- Security models and user access to applications
- Configuration of accounts for MetaFrame XP administrators
- Working with Novell Directory Services

General Configuration Issues

Citrix recommends that you do not use Windows primary domain controllers or backup domain controllers as MetaFrame XP servers, because of these factors:

- Domain controllers handle user validation for network logons and access to network resources. These functions and the associated network communication can significantly affect the performance of an application server.
- MetaFrame XP Setup cannot create anonymous accounts on primary or backup domain controllers, so you cannot publish applications for anonymous access on MetaFrame XP servers that are domain controllers.

Recommendations for Active Directory

If your network is configured to use Active Directory domains and groups, consider the following Citrix deployment recommendations:

**Use Windows 2000 or Windows Server 2003 servers.** Install MetaFrame XP exclusively on Windows 2000 or Windows Server 2003 servers. Native support for Active Directory is included in these versions of Windows, so you do not need to install additional services.
If users of the server farm use User Principal Name (UPN) logons, you must use Windows 2000 or higher servers exclusively, because UPN logons are not supported by Windows NT Server 4.0, Terminal Server Edition (TSE) servers, even with the Active Directory Services Interface installed. If the server farm contains both Windows 2000 and TSE servers, you must use the pre-Windows 2000 logon name in the format `domainname\username`.

**Use a single forest.** Install all servers in the server farm so they reside in one Active Directory forest. See “Using Active Directory Forests” on page 68.

**Install ADSI 2.5 or higher.** If you use TSE servers in the server farm, install Active Directory Services Interface (ADSI) 2.5 or higher on the TSE servers. ADSI significantly improves the speed of user enumeration in large domains. With ADSI, colored icons appear in directory lists to distinguish group types. Installing ADSI on all TSE servers and having Active Directory domains running in native mode lets you use domain local groups when publishing applications and allocating printers. In addition, ADSI lets TSE servers use LDAP queries rather than using legacy domain operations whenever possible.

If ADSI is not installed, TSE servers cannot enumerate domain local groups from Active Directory domains that are running in Active Directory native mode.

---

**Important** Even if a TSE server has ADSI installed, logging on using the User Principal Name (UPN) is not permitted for Program Neighborhood filtering. In addition, MetaFrame XP administrators cannot use a UPN to log on to the Management Console for MetaFrame XP. For this reason, you must use only Windows 2000 or later servers if you want users to log on with UPN credentials.

---

**Recommended Domain Configurations**

Citrix recommends the following for configuration of MetaFrame XP server farms with Active Directory:

- All servers reside in the same domain
- The server farm domain has no trust relationships with non-Active Directory domains
- The server farm is in a single Active Directory forest

These recommendations are not a requirement. However, multiple domains or trust relationships with non-Active Directory domains can affect all aspects of user authentication, which include:

- Authentication for MetaFrame XP administrators
- Access by users to published applications
Assignment of users to network printers

**Using Active Directory Forests**

If you use Windows Active Directory, Citrix recommends that all MetaFrame XP servers in a server farm belong to the same Active Directory forest. If your server farm has MetaFrame XP servers in more than one forest, users cannot log on using UPNs.

UPN logons use the format `username@UPN identifier`. With Active Directory, UPN logons do not require a domain to be specified, because Active Directory can locate full UPN logons in the directory. However, if multiple forests exist in the server farm, problems can arise because the same UPN identifier can exist in two domains in separate forests.

**Important** Because there is no efficient way to perform account resolution, MetaFrame XP does not support UPN logons if a MetaFrame XP farm spans multiple Active Directory forests.

**User Access to Applications and Printers**

To authorize user access to resources in a server farm, you select user and group accounts. For example, when you publish an application, you select the servers to host the application and the Management Console for MetaFrame XP lists the user accounts from the trust intersection of all the servers (accounts that are trusted by all the servers). You then select the users and groups that you want to allow to use the application.

After you select users, changing the list of host servers can change the trust intersection, which can make the application unavailable to users who are no longer in the servers’ trust intersection. If the trust intersection changes, the console informs you and removes users who are no longer eligible to use the resource from the authorized users list.

A published application is available only to users who can access every server that hosts the application. When multiple servers host the same application, you cannot predict which servers ICA Clients will connect to when they launch the application. Therefore, if a user is authorized to access only some servers, you cannot ensure that the user will always be able to use the application.

To prevent unpredictable access, MetaFrame XP removes users from the authorized users of a published application or printer if the accounts are not in the trust intersection for all the host servers.
Trust-Based Routing

Trust-based routing allows servers to be members of a server farm even if the servers belong to domains that don’t trust each other. In trust-based routing, a request to enumerate users or authenticate a user is routed to a server that has the required domain trust relationship if the originating server does not.

During a trust query cycle, a MetaFrame XP server registers its trusted domains with the server farm’s data store. This operation occurs during every service startup and approximately every six hours while the service is executing. Therefore, the data store is a central repository of all trust data for the servers in the server farm.

When a server needs to perform an operation (as defined below) on a domain that it doesn’t trust, the server determines from the data store which servers can perform the operation, and then routes the request to the most accessible server.

Trust-based routing applies to the following operations:

- Authenticating a MetaFrame XP administrator to the Management Console for MetaFrame XP
- Refreshing the display or launching an application in Program Neighborhood
-Enumerating users and groups in the console
- Resolving users and groups into distinguished account names when you add users or groups to a published application, add users to a printer auto-creation list, or define new MetaFrame XP administrators

Active Directory Security Model and Restrictions

Active Directory introduces new types of security groups to which network users can belong. You can use these security groups when you select users for published applications and network printers.

This section describes the Active Directory security groups and gives recommendations for using Active Directory security groups in a MetaFrame XP server farm.

Domain local groups. In the Active Directory model, domain local groups can contain groups from other domains, but the domain local group can be assigned to resources only in the domain in which it exists.

Universal groups. Universal groups can contain groups from other domains. Universal groups are stored in the Active Directory global catalog. Universal groups can be used for assigning permissions to resources in any domain.
Domain global groups. Global groups contain groups within the same domain and can be assigned to resources in any domain. Citrix recommends that you use domain global groups for user access to published applications and network printers.

Note Domain global groups are equivalent to non-Active Directory global groups.

Domain local groups and universal groups are available only in Active Directory domains that are operating in native mode.

If you plan to use universal groups or domain local groups, it is recommended that you follow the deployment guidelines in this section regarding domain configuration and use of groups to reduce administrative complexity.

For in-depth technical information about user access issues and configuration issues, see “User Permission Scenarios with Active Directory” on page 70.

If you change the servers that host a published application, the trust intersection with individual user accounts and with domain local groups can change.

For example, if all servers hosting an application or a printer reside in a common domain, D1, you can select domain local groups from D1 to grant access to the resource. If you then configure additional servers to host the resource and these servers do not reside in D1, the Management Console detects the change and removes the D1 domain local group from the configured accounts for the resource.

For more information about domains, establishing trust relationship among domains, and configuring user accounts in domains or Active Directory, see your Windows documentation.

User Permission Scenarios with Active Directory

With Active Directory, the following issues affect the choices you make when you configure a server farm and manage user permissions:

- If you use universal groups to give users permission to run published applications, all the servers that run an application (if you use Load Manager for load balancing) must reside in an Active Directory domain.

- If you use a domain local group to give users permission to run published applications, all servers that load-balance an application must belong to the same domain. Also, the domain local group you assign to an application must be in the common primary domain of all the load-balancing servers.

- If a user is a member of a domain local group, the group is in the user’s security token only when the user logs on to a machine in the same domain as the domain local group. Trust-based routing does not guarantee that a user’s logon request will be sent to a server in the same domain as the domain local group.
Chapter 3  Planning for MetaFrame XP Deployment

The table below describes how network configurations affect user permissions with Active Directory.

<table>
<thead>
<tr>
<th>Program Neighborhood filtering</th>
<th>Authenticating to published applications</th>
<th>Authenticating to the Management Console</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Domain Global Groups</strong></td>
<td>No adverse effects.</td>
<td>No adverse effects.</td>
</tr>
<tr>
<td><strong>Domain Local Groups</strong></td>
<td><strong>Recommendation:</strong> All servers in the farm must be in the same domain for Program Neighborhood filtering to work properly. <strong>Rationale:</strong> If a user is a member of a domain local group, the group is present in the user’s security token only when logging on to a machine in the same domain as the domain local group. Trust-based routing (see page 69) does not guarantee that a logon request will be sent to a server in the same domain as the domain local group. It guarantees only that the request will be handled by a server in a domain that trusts the user’s domain.</td>
<td><strong>Recommendation:</strong> All servers that load-balance an application must be in the same domain if a domain local group is authorized to use the application. <strong>Rationale:</strong> Domain local groups assigned to an application must be from the common primary domain of all the load-balancing servers. When you publish applications, domain local groups appear in the accounts list if the first condition above is met and accounts from the common primary domain are displayed (a green domain icon denotes the servers’ common primary domain). If a published application has users from any domain local groups and you add a server from a different domain, domain local groups are removed from the configured users list, because all servers must be able to validate any user with permission to run the application.</td>
</tr>
</tbody>
</table>
Supporting Novell Directory Service Users

This section covers the basic concepts and procedures for using MetaFrame XP with Novell Directory Service (NDS). For more detailed information about this topic, see Advanced Concepts for MetaFrame XP, available from the Support area of the Citrix Web site at http://www.citrix.com/support. Select Product Documentation.

MetaFrame XP supports user authentication through NDS. NDS offers access by a secure logon and organizes network resources in a directory tree for administration. When an NDS tree is designated in a MetaFrame XP server farm, the tree is accessed directly for NDS user account information.

You must install the Novell Client on MetaFrame XP servers used for NDS applications. Dedicate servers with the Novell Client to applications for NDS objects after NDS is enabled for a server farm. Do not host published applications assigned to Windows NT, Windows 2000, or Active Directory users on these servers. The server farm can be a mixture of servers used exclusively for NDS applications and other servers.

A MetaFrame XP administrator must have NDS credentials to manage applications and printers for NDS objects and to assign MetaFrame XP administrator privilege to NDS objects. To administer applications on a server dedicated to NDS, you must connect the Management Console to a server that has Feature Release 1 or higher.
The following table lists NDS terms and their meanings used in this section:

<table>
<thead>
<tr>
<th>Term</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tree</td>
<td>A set of objects set up hierarchically in a tree structure. The root object of the NDS tree is at the top of the tree.</td>
</tr>
</tbody>
</table>
| Container object    | The tree may or may not branch to these NDS Container objects:  
|                     | Country (a country location for this part of the organization)  
|                     | Organization (a company, university, or departmental unit)  
|                     | Organizational Unit (a business unit, division, or project team)                                                                     |
| Common Name         | The name for a leaf object on the tree. Examples of leaf objects are: users, groups, servers, and printers.                               |
| Context             | An object's position in the tree. One way to represent context is by a string of the Common Names of the objects in the path from the leaf or container object to the root. |
| Distinguished Name  | A combination of an object's common name and its context that makes up a complete NDS path for an object. A full Distinguished Name (DN) starts with a period, for the root, and has a period between each object name. |

**Setting up Support for NDS**

For MetaFrame XP to access NDS on Novell servers, one of the following must be installed:

- NDS Version 8.73 for NetWare 5.1
- NDS for eDirectory Version 8.5x for Windows NT 4.0, Windows 2000 Server, or NetWare 5.x

The minimum MetaFrame XP server software requirements are:

- Novell Client Version 4.8
- MetaFrame XP Feature Release 1 or higher

If you are setting up a server that does not yet have MetaFrame XP installed, install the Novell Client before you install MetaFrame XP. If MetaFrame XP is already installed, follow the procedure below for information about specifying the correct logon.

**Important** If you install the Novell Client on a MetaFrame XP server, set the following value in the [386Enh] section of the System.Ini file before you install MetaFrame XP:

FileSysChange=off
Make this change in System.ini for all users. If this parameter is not set correctly, the MetaFrame XP installer reports that the FileSysChange parameter is not valid. Novell technical document 10058117 refers to this issue. See the Novell knowledgebase on the Web at http://support.novell.com/search/kb_index.jsp for more information.

To change the registry on a server when the Novell Client is installed

If MetaFrame XP is installed before you install the Novell client, you must change registry settings on the server before and after you install the Novell Client.

**CAUTION** Using Registry Editor incorrectly can cause serious problems that can require you to reinstall the operating system. Citrix cannot guarantee that problems resulting from incorrect use of Registry Editor can be solved. Use Registry Editor at your own risk.

Make sure you back up the registry before you edit it. If you are running Windows NT, make sure you also update your Emergency Repair Disk.

1. **Before installing the Novell Client, run regedit32.**
2. **Edit the registry under:**
   
   HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon

   Double-click *GinaDLL*. In the *String Editor* window that pops up, type *Msgina.dll*, a new value for the GinaDLL entry.
3. **Install the Novell Client without restarting** when prompted.
4. **Edit the registry entry for GinaDLL as in Step 2. This time type Ctxgina.dll as the value.**
5. **With the key path for Winlogon still selected, click Edit on the top menu bar.**
6. **Click Add Value.**
7. **Type ctxGinaDLL in the Add Value dialog box. Data Type is REG_SZ.**
8. **Type nwgina.dll in the String Editor window. This is the new value for the new ctxGinaDLL entry.**
9. **Restart the server.**

To enable or disable NDS support for a server farm

NDS support is disabled for a server farm by default. MetaFrame XP supports one NDS tree per farm.
1. Connect to a server that has Feature Release 1 or higher and the Novell Client installed, using the version of the Management Console for MetaFrame XP released with Feature Release 1 or higher.

2. Right-click the farm node at the top of the tree and choose Properties.

3. Click MetaFrame XP Settings in the left pane of the Property sheet.

4. Enter the NDS tree name in the Novell Directory Services Preferred Tree field.

5. Click OK.

To assign MetaFrame XP administrator privileges to NDS objects

A MetaFrame XP administrator can assign MetaFrame XP administrator privileges to objects in an NDS tree, such as a country, organization, organization unit, group, user, or an alias.

1. Right-click MetaFrame XP administrators in the Management Console for MetaFrame XP and click Add MetaFrame XP Administrator.

2. On the first screen of the Add MetaFrame XP Administrator wizard, double-click to open the NDS tree. Objects in the NDS tree represent container objects and leaf objects.

3. Select the Show Users box to see the user and alias objects in this hierarchy.

4. Double-click to open container objects until the object that you want to add to the MetaFrame XP Administrator list is displayed in the dialog box. Select this object.

5. Click Add. Click Next.

6. Assign the tasks you want the MetaFrame XP administrator to be able to perform.

7. Click Finish.

This object and those below it have the selected MetaFrame XP administrator privileges.

To log on to the Management Console for MetaFrame XP as an NDS user

You need a Distinguished Name, password, and NDS tree name to perform the following steps. If you don’t have this information, consult the Novell or MetaFrame XP administrator who set up the NDS object to have MetaFrame XP administrator privileges.
1. Type a Distinguished Name in the **User Name** field. A full Distinguished Name starts with a period and has a period between each object name.

   For example, user JoeX, within two container objects (the Admin organization unit within the PNQ organization) would type the following Distinguished Name in the User Name box:

   `.JoeX.Admin.PNQ`

2. Type the password in the **Password** box.

3. Type the NDS tree name in the **Domain** box.

### To publish an application for NDS users

1. Log on to the Management Console for MetaFrame XP as an NDS user.

2. Verify that the intended host server has the Novell Client installed.

3. From the **Actions** menu, choose **New > Publish Application**.

4. Follow the instructions in the Publish Application wizard. Click **Help** to obtain detailed help for each step.

5. In the **Specify Users** dialog box of the Publish Application wizard, double-click to open the NDS tree.

6. Double-click to open container or leaf objects until the object to be granted access is in the window.

7. Select the object and click **Add**. Click **Finish**.

   The object and those under it can access the application.

### Configuring Printer Auto-Creation in NDS

The Management Console for MetaFrame XP can be used to choose Windows NT or Active Directory print queues and assign them to NDS objects for auto-creation. Print permissions to the queue must be granted to the Dynamic Local User created when NDS users log on to a server. This may involve enabling the Guest account on the print server. See Microsoft documentation for information about enabling the Guest account.

NDPS print queues cannot be chosen and assigned to NDS objects through Printer Management in the Management Console for MetaFrame XP. Consult Novell documentation for setting up NDPS print queues in ZENworks.

### Using the BUILTIN Group

When you specify users and groups for access to published applications or network printers, or when you create MetaFrame XP administrators, a special option, the BUILTIN group, is available from the menus that list network domains.
You can use the BUILTIN option:

- If your network environment is configured with Windows workgroups rather than with Windows network domains
- For compatibility with Novell’s ZENworks product

**Using BUILTIN for Publishing Applications and Printer Management**

If you use the BUILTIN group to specify users for applications and printer resources, do not use Program Neighborhood and the Web Interface for ICA Client connections to published applications. Use only custom ICA connections in Program Neighborhood to launch applications.

**Compatibility with ZENworks Dynamic Local Users**

In network environments that use Novell’s ZENworks product for user management, use the BUILTIN group for compatibility. You select the BUILTIN group to specify dynamic local users managed by ZENworks when you publish applications and assign users to network printers.

With ZENworks, the software that handles user logons (called GINA for Graphical Identification and Authentication) on every machine that supports this feature is replaced with the GINA provided by Novell. Users log on by entering Novell Directory Service (NDS) credentials. An NDS server authenticates the user and determines permissions for the logon server. On this server, ZENworks dynamically creates a local user and gives group permissions according to the user policies. The only constant security IDs between sessions are the security IDs of the BUILTIN groups to which the NDS user belongs.

**Changing Domain Trust Relationships**

If you add a new domain trust relationship, you might be unable to select user accounts in the server farm based on the trust relationship right away.

You might see this situation when you publish an application, for example, after adding a new trust relationship. In the dialog box where you configure user accounts for the application, when you select a domain, the newly-trusted domain does not appear until the IMA Service propagates the new trust relationship throughout the server farm.

The user management subsystem updates its domain trust information every six hours (and during service startup). Therefore, it might take as long as six hours for all servers in the server farm to recognize a new trust relationship.
You can avoid a delay in detection of network trust changes by restarting the IMA Service on all servers affected by the change. For example, if you change a trust relationship to allow DomainX to trust DomainY, restart all servers that belong to DomainX. With Active Directory, if you add a new domain to an Active Directory forest, for example, restart the IMA Service on all servers that belong to a domain in the forest that is affected by the change.

If you are unsure which servers are affected by a trust relationship change, you can restart the IMA Service on all servers in the farm to ensure that the change is recognized. Citrix recommends that you restart the IMA Service only during off-peak hours when the load on the servers is very low.

### Configuring MetaFrame XP Administrator Accounts

MetaFrame XP administrators manage MetaFrame XP server farms. You can create MetaFrame XP administrator accounts with the following permission levels:

- **Full administration rights to all areas of MetaFrame XP server farm management.**
- **View-only access to all areas of server farm management.**
- **Mixed levels of access to areas of farm management or specific tasks within those areas; administrators can have a mixture of view-only access, write access, or no access.**

When you install the first MetaFrame XP server in a new server farm, you specify an initial farm administrator. This user account is automatically configured as a MetaFrame XP administrator with full administration rights in the Management Console for MetaFrame XP.

To give other user accounts access to the console, a MetaFrame XP administrator with full administration rights logs on to the console and creates other MetaFrame XP administrator accounts. The level of permission for various areas of farm management depends on the specific business function of the administrator. For example, your system or network administrators may need complete access to all areas of farm and server management, while help desk personnel may need only view access to most areas.

To give administrators of your server farm access to the Management Console, you add their network user accounts to the MetaFrame XP administrators group in MetaFrame. The console uses standard Windows network logon and user account authentication mechanisms. Click the MetaFrame XP Administrators node in the left pane of the console to view all MetaFrame XP administrators.
When you create a MetaFrame XP administrator account for a user, you can grant or deny access to specific MetaFrame XP tasks, such as disconnecting users, or to an entire area of server farm management, such as managing sessions. You can create specialized MetaFrame XP administrators with the permission level to carry out specific tasks without granting these administrators full access to all areas of farm management.

For more information about delegating administration rights to MetaFrame XP administrators, see “Configuring MetaFrame XP Administrator Accounts” on page 174.

**Note**  One MetaFrame XP administrator account with full administration rights must always exist in the server farm. MetaFrame XP prevents you from deleting the last MetaFrame XP administrator account with this level of permission. However, if the account no longer exists in the network account authority, the console allows a local administrator to log on to the console to set up MetaFrame XP administrator accounts.

---

**Planning for Client and Server Communications**

In a MetaFrame XP server farm, several types of data transmission and communication pathways link ICA Clients with MetaFrame XP servers and other components.

Consider the following communication issues for your deployment of MetaFrame XP, ICA Clients, and optionally, the Web Interface for MetaFrame XP and related Citrix services:

- Configuring ICA browsing so ICA Clients can find published applications and MetaFrame XP servers in your server farm
- Configuring network firewalls to allow communication among ICA Clients, MetaFrame XP, and the Web Interface
- Configuring a MetaFrame XP server farm for interoperability with MetaFrame 1.8

The first part of this section focuses on MetaFrame XP. For information about communication issues with MetaFrame XP and MetaFrame 1.8, see “ICA Browsers and MetaFrame 1.8 Interoperability” on page 93.
**Note** Features described in this section, including ICA browsing and published applications, are not available to all ICA Clients. This section focuses on the Version 6.0 and later ICA Win32 Client features and server farm configuration with this client. For information about server connections options in other clients, see the *Citrix ICA Client Administrator’s Guide* for the clients you plan to deploy.

### Linking ICA Clients and MetaFrame XP Servers

In a server farm, the main communication processes between ICA Clients and MetaFrame XP servers are ICA browsing and ICA sessions.

*ICA Clients perform ICA browsing when requesting applications from MetaFrame XP servers. A client initiates an ICA session with the server to run an application.*

### ICA Browsing

*ICA browsing* is a process in which an ICA Client transmits data to locate MetaFrame servers on the network and get information about the server farm’s published applications.

For ICA browsing, clients communicate with the Citrix XML Service or the ICA Browser, depending on the browsing protocol selected in the ICA Client. These options are described under “Configuring ICA Browsing” on page 81.

ICA browsing occurs when:

- Users launch published applications. The ICA Client sends a request to locate the application on a MetaFrame XP server. If you are using Load Manager, a component of MetaFrame XPe or XPa, the client gets the address of the server with the lightest load.
- Program Neighborhood users display the Application Set list in the Find New Application Set wizard.
- Program Neighborhood users display the **Server** or **Published Application** list in the Add New ICA Connection wizard to create a custom ICA connection.
ICA Sessions

An ICA session is the communication link between ICA Clients and MetaFrame XP servers that ICA Clients establish to run applications. In an ICA session, a MetaFrame XP server transmits an application’s screen display to the client, and the ICA Client sends the user’s keystrokes, mouse actions, and local data to the application running on the server.

The default port on MetaFrame XP servers for ICA sessions is 1494. This port must be open on firewalls for inbound communication if ICA Clients are outside the firewall. The port used on the client for the ICA session is configured dynamically when the session is established.

In addition to MetaFrame XP servers, other components, such as servers running the Web Interface for MetaFrame XP, proxy servers, and Web browsers can be involved in establishing ICA sessions. In all cases, the basic communications link for an ICA session is between the ICA Client and MetaFrame XP server.

Configuring ICA Browsing

Users connect to servers and applications from application sets or custom ICA connections in the ICA Client. As described above, ICA browsing is a process that locates MetaFrame XP servers and published applications in response to requests from an ICA Client.

- When a user launches an application from an application set, ICA browsing locates a server that hosts the published application so the ICA Client can connect to the server and run the application.

- When a user sets up a custom connection, ICA browsing produces a list of published applications or servers in the server farm. The user selects an application or server to define the custom connection.

**Important** MetaFrame XP does not support multiple farms on the same subnet configured to respond to Master Browser requests.
Server Location Settings

The method that ICA Clients use for ICA browsing depends on the specified server location settings. Users running Program Neighborhood can configure server location settings using the Program Neighborhood user interface.

- For new application sets and custom connections, you configure server location settings from the Server Location button in the Find New Application Set wizard and Add New ICA Connection wizard in the ICA Client.
- For existing application sets and custom ICA connections, you can change Server Location settings on the Connection tabs in the Settings dialog boxes.

Note Some ICA Clients do not use ICA browsing and connect only to specified servers. The options described in this section are for the ICA Win32 Client. For information about other server location options, see the Citrix ICA Client Administrator’s Guides for the clients you plan to deploy.

Specifying the Network Protocol for ICA Browsing

The Network Protocol setting you specify for server location in the ICA Client affects the following deployment issues related to ICA browsing:

- The communications protocol the client uses to locate servers
- The MetaFrame XP component the client communicates with
- The port the client communicates with
- The default locations the client contacts
Using TCP/IP+HTTP Network Protocol for ICA Browsing

Citrix recommends that you select TCP/IP+HTTP as the server location network protocol in the ICA Client. In addition, Citrix recommends that you specify servers to contact for ICA browsing by entering IP addresses or DNS names of MetaFrame XP servers in the Address List box.

When TCP/IP+HTTP is selected and you specify MetaFrame XP servers in the Address List box, the ICA Client communicates with the Citrix XML Service on a specified server for ICA browsing.

By default, if no server is specified, the client attempts to resolve the name “ica” to an IP address. This is indicated by the virtual server location “ica” in the Address List box. This feature allows the DNS or WINS administrator to configure a host record that maps “ica” to a valid MetaFrame XP server IP address that can service XML requests from ICA Clients.

Tip You can configure the ICA Clients’ DNS server to use round-robin DNS to map the name “ica” to a set of MetaFrame XP servers that can service the XML requests. This is a convenient method to use to avoid individual configuration of server location addresses on ICA Clients.

To locate the Citrix XML Service, the ICA Client makes an HTTP connection to port 80 on the MetaFrame XP server. If the user is launching a published application, for example, the XML Service then sends to the client the address of a MetaFrame XP server that has the application published.

When you configure the ICA Client to use TCP/IP+HTTP, communication between the client and XML Service consists of XML-formatted data in HTTP packets.

Citrix recommends using TCP/IP+HTTP protocol for ICA browsing because it provides several advantages for most server farms:

• TCP/IP+HTTP uses XML data encapsulated in HTTP packets, which the client sends to port 80 by default. Most firewalls are configured so port 80 is open for HTTP communication.

• TCP/IP+HTTP does not use UDP (User Datagram Protocol) or broadcasts to locate servers in the server farm.

• Routers pass TCP/IP packets between subnets, which allows ICA Clients to locate servers that are not on the same subnet.
Using TCP/IP Network Protocol for ICA Browsing

If TCP/IP is specified as the server location network protocol and (Auto-Locate) appears in the Address List box, ICA Clients send UDP broadcasts to the ICA Browser service on port 1604 to locate MetaFrame XP servers and published applications.

By default, MetaFrame XP server farms operating in native mode do not respond to ICA Clients that use UDP broadcasts for ICA browsing. Therefore, if clients are configured to use TCP/IP and to auto-locate servers, they will fail to locate MetaFrame XP servers or published applications in the server farm.

You can use two configurations for MetaFrame XP servers to respond to ICA Client broadcasts for ICA browsing:

- You can set the MetaFrame XP server farm to operate in mixed mode for interoperability with a MetaFrame 1.8 server farm as you migrate the farm to MetaFrame XP.
- You can set the MetaFrame XP server farm, or individual MetaFrame XP servers, to respond to ICA Client broadcasts for compatibility with deployed clients.

When a MetaFrame XP server farm operates in mixed mode, by default only MetaFrame XP servers that are master ICA Browsers respond to UDP broadcasts from ICA Clients. For more information about mixed mode operation, see “ICA Browsers and MetaFrame 1.8 Interoperability” on page 93. For information about data collectors, see “Configuring Zones and Data Collectors” on page 189. For information about configuring server response to broadcasts, see “Setting up Response to ICA Client Broadcasts” on page 184.

Because UDP broadcast packets do not traverse subnets, using broadcasts for ICA browsing works only if a server that responds to broadcasts is in the same subnet as the clients. After the ICA Client locates a server, it communicates using directed (not broadcast) UDP to port 1604.

Because of broadcast limitations, you might prefer to enter one or more IP addresses or DNS names of MetaFrame XP servers in the Address List box. You must do this if the ICA Client is not on the same subnet as a data collector.

In summary, using the TCP/IP setting and auto-location for ICA browsing is less efficient than using TCP/IP+HTTP because it relies on UDP and UDP broadcasts.
Effects of Server Location Settings on ICA Browsing

The following table summarizes ICA browsing methods that result from various Network Protocol and Address List settings.

<table>
<thead>
<tr>
<th>Network protocol</th>
<th>Address list</th>
<th>Data type</th>
<th>Responder</th>
<th>Farm configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td>TCP/IP+HTTP</td>
<td>Default (&quot;ica&quot;)</td>
<td>XML / HTTP</td>
<td>XML Service</td>
<td>Native mode or mixed mode.</td>
</tr>
<tr>
<td>TCP/IP+HTTP</td>
<td>Specified server(s)</td>
<td>XML / HTTP</td>
<td>XML Service</td>
<td>Native mode or mixed mode. In mixed mode, specify MetaFrame XP servers.</td>
</tr>
<tr>
<td>TCP/IP</td>
<td>Default (Auto-Locate)</td>
<td>UDP broadcast</td>
<td>ICA Browser on data collectors</td>
<td>Mixed mode. Native mode if servers are set to respond to broadcasts. Servers must be on clients' subnet.</td>
</tr>
<tr>
<td>TCP/IP</td>
<td>Specified server(s)</td>
<td>Directed UDP</td>
<td>ICA Browser</td>
<td>Native or mixed mode.</td>
</tr>
</tbody>
</table>

Communicating with the Citrix XML Service

Citrix XML Service is a MetaFrame XP server component. The service is installed by default on all MetaFrame XP servers. It is also installed with Feature Release 1 for MetaFrame 1.8.

When ICA Clients are configured to use TCP/IP+HTTP for ICA browsing, the XML Service communicates published application information to clients using HTTP protocol and XML data. The XML service also communicates published application information to servers running the Web Interface for MetaFrame XP.

For example, when a user launches a published application in Program Neighborhood, the ICA Client sends a request for the application. The XML Service responds with the address of a MetaFrame XP server on which the application is published.

With the Web Interface for MetaFrame XP, for example, a user connects to a Web page using a Web browser. The XML Service provides a list of available applications to the server running the Web Interface. The Web server displays the available applications on the user’s personalized application Web page.

Setting the Port for Citrix XML Service

The Citrix XML Service uses an IP port on the MetaFrame XP server for communication with ICA Clients and the Web Interface for MetaFrame XP. You can set the port number during or after MetaFrame XP setup.

Important All MetaFrame XP servers in the server farm must use the same port for the XML service.
The XML Service default communication port is 80. Port 80 is open on most firewalls to allow inbound communication to Web servers. If your MetaFrame XP and Web servers are behind a firewall, this port is probably open, allowing ICA Clients to communicate with MetaFrame XP servers and allowing Web browsers to communicate with servers running the Web Interface.

If you intend to send data over a secure HTTP connection using SSL, be sure that the XML Service is set to share its port with IIS and that IIS is configured to support HTTPS.

**Note**  
Port 80 is the default port for HTTP communication with Web servers. The Citrix XML Service includes an Internet Server Application Programming Interface (ISAPI) extension that you can plug into Internet Information Services (IIS). The extension allows IIS and the XML Service to share port 80. This is necessary only if IIS is installed on MetaFrame XP servers. IIS is required to run the Web Interface for MetaFrame XP. The default MetaFrame XP installation installs the Web Interface if IIS is installed on the server. However, for best performance, Citrix recommends that IIS and the Web Interface be installed on separate dedicated Web servers.

For information about configuring the XML Service port number, see “Configuring the Citrix XML Service Port” on page 125. For information about configuring the port that the Web Interface uses, see the *Web Interface for MetaFrame XP Administrator’s Guide*.

**Important**  
If you change the port used by the Citrix XML Service, you must set the correct port in the ICA Client. You can specify a port number when you add a server to the Address List under Server Location in the ICA Client. If you also use the Web Interface, be sure it uses the correct port for XML Service communication. For more information, see the Web Interface documentation. See the *Citrix ICA Client Administrator’s Guide* or the client’s online help for instructions on configuring ICA Clients.

**Using DNS Address Resolution**

ICA Client browsing requests normally generate an IP address for connecting to MetaFrame XP servers. You can configure MetaFrame XP servers to respond with the fully qualified domain name (FQDN). This feature, called Domain Name System (DNS) address resolution, is available to clients using the Citrix XML Service.
MetaFrame XP servers reply with an IP address as the default. You can change the default setting, which applies to the entire server farm, in the Management Console for MetaFrame XP. In most situations, using IP addresses works well and requires less overhead.

For ease of administration, ICA Clients have a client file that is already configured to request FQDNs if DNS addressing is enabled in the server farm. ICA Clients connecting through the Web Interface request IP or DNS addresses based on a line in a Web server configuration file. This file is set up for IP addresses initially. Regardless of what ICA Clients are set up to request, unless DNS addressing is enabled for the server farm, IP addresses are returned.

DNS address resolution works only in a native mode MetaFrame XP server farm and you must be using ICA Client 6.20.985 or later.

**Important** If DNS addressing is enabled, clients cannot connect reliably unless they can resolve the fully qualified domain name of all servers in the server farm. Ping a server with its DNS host name to verify this. Unless your DNS environment is configured specifically to use this feature, Citrix recommends that you do not enable DNS address resolution in the server farm.

### To enable or disable DNS address resolution in a server farm

1. Open the Management Console for MetaFrame XP.
2. Right-click the farm node at the top of the tree and choose **Properties**.
3. Select **MetaFrame XP Settings** in the left pane of the farm’s Properties sheet.
4. On the right pane of the Properties sheet, select or clear **Enable XML Service DNS address resolution**.
5. Click **OK**.

### Configuring Network Firewalls

Protecting servers that contain valuable data and are critical to your organization’s mission requires that you consider security as an integral part of your MetaFrame XP deployment planning.

In addition to physically securing servers, most organizations will install network security measures including firewalls to isolate MetaFrame XP servers and Web browsers from the Internet and from publicly accessible networks.

To deploy MetaFrame XP servers behind network firewalls, configure access for ICA Client users by allowing packets to pass to specific communication ports that ICA Clients and other MetaFrame XP components use.
As described above, Citrix recommends that ICA Clients use TCP/IP+HTTP for ICA browsing. To use this protocol with clients outside a firewall, configure the firewall to pass inbound HTTP packets on port 80, the default port for the Citrix XML Service on MetaFrame XP servers. This port is usually open on firewalls for inbound HTTP packets to Web servers.

In ICA sessions, ICA Clients communicate with port 1494 on MetaFrame XP servers. If the clients are outside the firewall, this port must be open for inbound communication to MetaFrame XP servers.

### Server Farm Configurations

The diagrams below illustrate network configurations for MetaFrame XP server farms. The diagrams identify port numbers, components, and the recommended protocol for ICA browsing. See “Configuring ICA Browsing” on page 81 for more information.

In the diagrams in this section, communication paths are bidirectional; arrows indicate the direction in which communication is initiated.

The first diagram shows the basic configuration for communication between ICA Client and MetaFrame XP server when a user launches a published application.
The process of running the application begins with ICA browsing (server location). TCP/IP+HTTP protocol and server addresses are specified for server location in the ICA Client.

1. The client sends a request to the Citrix XML Service on port 80 on a specified server using HTTP.

2. The Citrix XML Service sends the address of a server that has the requested application.

3. The ICA Client establishes an ICA session with the MetaFrame XP server specified by the XML Service. ICA packets travel from the client to port 1494 on the server. ICA packets travel from the server to a dynamically assigned port number on the client.

Organizations often place their Web servers in a demilitarized zone (DMZ) between firewalls. In the configuration shown below, servers running the Web Interface for MetaFrame XP are between firewalls to isolate them from the MetaFrame XP server farm and ICA Clients.
As with the basic configuration, Citrix recommends ICA Clients use TCP/IP+HTTP protocol to communicate through a firewall. When the user launches an application from a Web page, the ICA Client establishes an ICA session through the firewall to port 1494 on the MetaFrame XP server.
The diagram above illustrates communication between the ICA Client and MetaFrame XP server when SSL encryption is used.

The process of running the application begins with ICA browsing (server location). In this scenario, SSL+HTTPS protocol and server IP addresses are specified for server location in the ICA Client.

1. The client sends an encrypted request to the Citrix SSL Relay on port 443 on a specified server using HTTPS.
2. The SSL Relay decrypts the request and sends it to the Citrix XML Service on port 80.
3. The Citrix XML Service sends the address of a server that has the requested application to the SSL Relay.
4. The SSL Relay encrypts and sends the address of the server to the ICA Client.
5. The ICA Client establishes an SSL-encrypted ICA session with the MetaFrame XP server specified by the Citrix XML Service. ICA packets travel from the client to port 443 on the server and are then decrypted and passed to port 1494. SSL-encrypted ICA packets travel from the server to the client.
## Configuring TCP Ports in MetaFrame XP Server Farms

The table below lists the TCP/IP ports that MetaFrame XP servers, ICA Clients, the IMA Service, and other Citrix services use in a server farm. This information can help you configure firewalls and troubleshoot port conflicts with other software. The table includes configuration information when you can change default settings.

<table>
<thead>
<tr>
<th>Communication</th>
<th>Default port</th>
<th>Configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td>ICA sessions (ICA Clients to MetaFrame XP servers)</td>
<td>1494</td>
<td>See &quot;ICAPORT&quot; on page 347 for instructions about changing the port number. This port must be open on firewalls for inbound packets from ICA Clients to MetaFrame XP servers.</td>
</tr>
<tr>
<td>Citrix XML Service</td>
<td>80</td>
<td>This port must be open on firewalls for inbound packets when ICA Clients use the TCP/IP+HTTP network protocol for server location. See &quot;Configuring the Citrix XML Service Port&quot; on page 125 for configuration instructions.</td>
</tr>
<tr>
<td>Citrix SSL Relay</td>
<td>443</td>
<td>See &quot;Step 3 - Changing the SSL Port&quot; on page 166 for configuration instructions.</td>
</tr>
<tr>
<td>MetaFrame XP server-to-server</td>
<td>2512</td>
<td>See &quot;MetaFrame XP Commands&quot; on page 311 for information about the IMAPORT command.</td>
</tr>
<tr>
<td>MetaFrame XP server to Microsoft SQL or Oracle server</td>
<td>139, 1433, or 443 for MS-SQL</td>
<td>See the documentation for your database software.</td>
</tr>
<tr>
<td>The Management Console-to-MetaFrame XP server</td>
<td>2513</td>
<td>See &quot;MetaFrame XP Commands&quot; on page 311 for information about the IMAPORT command.</td>
</tr>
<tr>
<td>ICA Clients to ICA Browser service (UDP)</td>
<td>1604</td>
<td>MetaFrame XP servers always respond to directed UDP requests. See &quot;Setting up Response to ICA Client Broadcasts&quot; on page 184 for enabling MetaFrame XP servers to respond to broadcasts.</td>
</tr>
<tr>
<td>Server-to-Server (directed UDP)</td>
<td>1604</td>
<td>Not configurable. This port is used only when the farm is operating in mixed mode with MetaFrame 1.8 servers.</td>
</tr>
</tbody>
</table>
ICA Browsers and MetaFrame 1.8 Interoperability

This section describes issues related to ICA browsing when MetaFrame XP operates in mixed mode with a MetaFrame 1.8 server farm. For more information about selecting mixed mode and issues related to interoperability, see “Interoperability with MetaFrame 1.8” on page 100.

If you configure a MetaFrame XP server to use mixed mode, two separate farms—one that contains only MetaFrame 1.8 servers and one that contains only MetaFrame XP servers—act together so they appear to ICA Clients as one server farm.

When MetaFrame XP is in mixed mode, the two farms appear unified because ICA Browsers in each farm pool information and a MetaFrame XP server becomes the master browser of both farms. The master browser holds information about the published applications available on each server.

**Note** The ICA Browser is a system service on MetaFrame 1.8 servers. On MetaFrame XP servers, the ICA Browser is a subsystem of the IMA Service that can respond to ICA Client broadcasts. In this chapter, references to the ICA Browser apply to both the MetaFrame 1.8 browser service and the MetaFrame XP browser function.

In a MetaFrame 1.8 server farm, when a user launches a published application, the ICA Client asks the master ICA Browser for the address of a server that can run the application. The ICA Client also uses the master browser to find new application sets and to list servers and published applications for custom connections.

In mixed mode, ICA Clients can communicate with the single master browser for the interoperating server farms by connecting to MetaFrame XP servers in either farm. A client can contact the master browser through the ICA Browser using TCP/IP network protocol.

When you select mixed mode operation, you enable a MetaFrame XP farm to respond to broadcasts from ICA Clients that use TCP/IP and auto-location of servers. By default, only the master ICA Browser and RAS servers respond to broadcasts in mixed mode; the per-server option to respond to broadcasts is disabled.

For more information about ICA browsing methods that involve broadcasts, see “Configuring ICA Browsing” on page 81.

When ICA Clients use TCP/IP+HTTP for server location, they do not send broadcasts during ICA browsing and the Citrix XML Service, rather than the ICA Browser, responds to the clients as mentioned above.
Citrix recommends you configure ICA Clients to use TCP/IP+HTTP and that you specify one or more servers in the Address List. The servers you specify must have the XML service to respond to ICA browsing. The Citrix XML Service is not available on MetaFrame 1.8 servers without Feature Release 1.

**Election of the Master ICA Browser**

When a MetaFrame XP server farm operates in mixed mode, the ICA Browser runs on every server. A MetaFrame XP server takes over as the master ICA Browser for the MetaFrame 1.8 server farm and the MetaFrame XP server farm and stores information about both server farms.

The master ICA Browser is chosen by a master browser election. The ICA Browser system elects a master browser when:

- The master browser does not respond to another ICA Browser
- The master browser does not respond to an ICA Client
- A MetaFrame server is started
- Two master browsers are detected on the same network subnet

A set of election criteria is used to choose a master browser. An ICA Browser starts a browser election by broadcasting its election criteria. If another browser has a higher election criteria, it broadcasts its own election criteria. Otherwise, the last ICA Browser to respond to the election becomes the master browser.

The following criteria, in order, determine the master browser:

- Latest ICA Browser version
- Master browser designation by Citrix Server Administration or registry key
- Domain controller
- Longest ICA Browser up time
- MetaFrame server name in alphabetical order

For example, a MetaFrame server that has a later version of the ICA Browser Service wins election as master browser over a server that has a longer up time for the ICA Browser Service. Because the ICA Browser in MetaFrame XP is a later version than the MetaFrame 1.8 ICA Browser, a MetaFrame XP server in most cases becomes the master browser when server farms are in mixed mode.

**Note** If a MetaFrame XP server has **Do not attempt to become the master ICA Browser** selected, it does not participate in master browser elections.
You can use the `query server` command to discover the MetaFrame server acting as the master browser. The `query server` command displays all servers on each network transport (TCP/IP, IPX, and NetBIOS). An `M` next to the network address of a server indicates that it is the master browser for that network transport. A `B` indicates a backup browser. A `G` indicates a gateway between subnets in the MetaFrame 1.8 server farm.

**Changing Server Drive Letters**

MetaFrame XP’s *client drive mapping* gives ICA Client users access to their local drives when they use applications on MetaFrame XP servers. When users start ICA sessions, MetaFrame XP assigns drive letters to client drives.

- Client drives that use the same letters as the server’s drives are assigned different drive letters, starting with V and going backwards through the alphabet.

- If client drive letters do not conflict with the server’s drive letters, MetaFrame XP uses the original letters for client drives.

- Server floppy disk drives are not available to client users, so MetaFrame XP uses the drive letters for floppy disk drives specified on the client devices. Non-Windows ICA Clients that support floppy drive mapping can be configured manually with specific drive letter mappings for each drive.

Default drive mappings for sessions are shown in the following table. Client drives C and D are renamed V and U, because the server drives use the letters C and D.

<table>
<thead>
<tr>
<th>Logical drive letter</th>
<th>Drive letter in ICA sessions</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Client drives</strong></td>
<td></td>
</tr>
<tr>
<td>A (floppy drive)</td>
<td>A</td>
</tr>
<tr>
<td>B (floppy drive)</td>
<td>B</td>
</tr>
<tr>
<td>C</td>
<td>V</td>
</tr>
<tr>
<td>D</td>
<td>U</td>
</tr>
<tr>
<td><strong>Server drives</strong></td>
<td></td>
</tr>
<tr>
<td>C</td>
<td>C</td>
</tr>
<tr>
<td>D</td>
<td>D</td>
</tr>
<tr>
<td>E</td>
<td>E</td>
</tr>
</tbody>
</table>
To make drive access more familiar for client users, you can change the server drives to use letters that are not likely to be used by client devices. Doing so ensures that client drives retain their original drive letters. The following table shows an example of drive letters used if you change the drive letters of a MetaFrame XP server.

<table>
<thead>
<tr>
<th>Logical drive letter</th>
<th>Drive letter in ICA sessions</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Client drives</strong></td>
<td></td>
</tr>
<tr>
<td>A (floppy drive)</td>
<td>A</td>
</tr>
<tr>
<td>B (floppy drive)</td>
<td>B</td>
</tr>
<tr>
<td>C</td>
<td>C</td>
</tr>
<tr>
<td>D</td>
<td>D</td>
</tr>
<tr>
<td><strong>Server drives</strong></td>
<td></td>
</tr>
<tr>
<td>C</td>
<td>M</td>
</tr>
<tr>
<td>D</td>
<td>N</td>
</tr>
<tr>
<td>E</td>
<td>O</td>
</tr>
</tbody>
</table>

**CAUTION**  If you intend to change a server’s drive letters, do so before you install MetaFrame XP. If you change server drive letters after MetaFrame XP installation, you must do it before installing any applications.

If you change the server’s drive letters, MetaFrame XP searches the following registry keys and changes all drive references to reflect the new drive letters:

- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\*
- HKEY_LOCAL_MACHINE\SOFTWARE\Classes\*
- HKEY_LOCAL_MACHINE\SOFTWARE\Equinox\eqn\CurrentVersion\NetRules
- HKEY_LOCAL_MACHINE\SYSTEM\*
- HKEY_CLASSES_ROOT\*
- HKEY_USERS\*

MetaFrame XP also updates the pagefile entry and the following shortcut files:

- %SystemRoot%\Profiles\Default User\*.lnk
- %SystemRoot%\Profiles\Administrator\*.lnk
- %SystemRoot%\Profiles\All Users\*.lnk

The first time a user logs on to the MetaFrame XP server after you change the drive letters, references to the old drive letters in the user’s profile are updated.

Run Driveremap.exe to change the server’s drive letters. For more information about this utility, see “DRIVEREMAP” on page 338.
Using Smart Cards with MetaFrame XP

You can use smart cards in your MetaFrame XP environment. Smart cards are small plastic cards with embedded computer chips. Smart cards can contain memory only, memory with security logic, or memory with CPU capabilities, depending on the intended application.

In a business computer network setting, smart cards are an effective implementation of public-key technology and can be used to:

- Authenticate users to networks and computers
- Secure channel communications over a network
- Use digital signatures for securing content

If you are using smart cards for secure network authentication, your users can authenticate to applications and content published on MetaFrame XP servers. In addition, smart card functionality within these published applications is also supported.

For example, a published Microsoft Outlook application can be configured to require that users insert a smart card into a smart card reader attached to the client device to log on to the MetaFrame XP server. After users are authenticated to the application, they can digitally sign email using certificates stored on their smart cards.

Citrix has tested smart cards that meet Standard 7816 of the International Organization for Standardization (ISO) for cards with electrical contacts (known as a contact card) that interface with a computer system through a device called a smart card reader. The reader can be connected to the host computer by the serial, USB, or PCMCIA port.

Citrix supports the use of PC/SC-based cryptographic smart cards. These cards include support for cryptographic operations such as digital signatures and encryption. Cryptographic cards are designed to allow secure storage of private keys such as those used in Public Key Infrastructure (PKI) security systems. These cards perform the actual cryptographic functions on the smart card itself, meaning the private key and digital certificates never leave the card.

In addition, you can use two-factor authentication for increased security. Instead of merely presenting the smart card (one factor) to conduct a transaction, a user-defined PIN (a second factor), known only to the user, is used to prove that the cardholder is the rightful owner of the smart card.

**Note** MetaFrame XP does not support RSA Security Inc.’s PKCS (Public-Key Cryptography Standard) #11 functional specification for personal cryptographic tokens.
You can also use smart cards with the Web Interface for MetaFrame XP. For details about configuring the Web Interface for smart card support, see the *Web Interface for MetaFrame XP Administrator’s Guide*, located in the Docs directory on the MetaFrame XP Server CD.

**Software Requirements**

The following section presents the basic guidelines for using smart cards with MetaFrame XP. Consult your smart card vendor or integrator to determine detailed configuration requirements for your specific smart card implementation.

The following components are required on the MetaFrame XP server:

- PC/SC software
- Cryptographic Service Provider (CSP) software

These components are required on the device running the supported ICA Client:

- PC/SC software
- Smart card reader software drivers
- Smart card reader

Your Windows server and client operating systems may come with PC/SC, CSP, or smart card reader drivers already present. See your smart card vendor for information about whether these software components are supported or must be replaced with vendor-specific software.

If you are using Pass-Through Authentication to pass credentials from your Windows 2000 or Windows XP client computer to the smart card server session, CSP software must be present on the client computer.

You do not need to attach the smart card reader device to your server during CSP software installation if you can install the smart card reader driver portion separately from the CSP portion.

**Configuring the Server**

A complete and secure smart card solution can be relatively complicated and Citrix recommends that you consult your smart card vendor or integrator for details. Configuration of smart card implementations and configuration of third-party security systems such as certificate authorities are beyond the scope of this documentation.

Smart cards are supported for authenticating users to published applications, or for use within published applications that offer smart card functionality. Only the former is enabled by default upon installation of MetaFrame XP.
To enable support for smart card usage within an application, run the Scconfig.exe command line utility on each MetaFrame XP server that hosts the application. This utility is used to specify the applications (for example, Outlook.exe) that you want to configure to have smart card transactions redirected from the server on which they execute to the client device that hosts the smart card reader. This utility may be executed remotely by specifying a target server according to the syntax below.

```
SCCONFIG /?
SCCONFIG ([/SERVER:servername] | [/FARM]) ([/QUERY] | [/Q])
SCCONFIG [/SERVER:servername] [/INHERIT:on|off]
```

The parameters used in this utility are explained below.

- The /? option returns on-screen help for this utility.
- The /SERVER:servername option specifies the target server to configure.
- The /FARM option is used to set a farm-wide setting but will not configure any servers. When the farm-wide setting is set, servers are configured according to the state of the /INHERIT option. When MetaFrame XP is installed on the server, “on” is the default state for /INHERIT.
- If neither /SERVER or /FARM option is specified, the local server is assumed.
- The /QUERY or /Q option can be used with the /SERVER or /FARM option to display currently configured settings.
- The /LOGON option is used to turn on or off support for smart card authentication during MetaFrame XP server logon. Upon MetaFrame XP server installation, “on” is the default state for /LOGON.
- The /ENABLE_PROCESS and /DISABLE_PROCESS options are used to enable or disable support for applications that can take advantage of smart card functionality when run as published applications. For example, to enable support for Microsoft Outlook, the processname would be OUTLOOK.EXE.

### Setting Windows Policies for Smart Cards

Windows supports two security policy settings for interactive logon to a server session. ICA Client sessions can utilize the following policies:

- **Require smart card for interactive session logon.** This policy is a user policy that requires the user to insert a smart card for authentication.
• **Smart-card removal policy.** This policy is a computer policy that has three possible settings to determine the client device behavior when the user removes the smart card from the smart card reader:
  - None (no effect)
  - Lock Workstation (disconnects all MetaFrame XP user sessions)
  - Force Logoff (logs off all MetaFrame XP user sessions)

**Configuring the Client**

The following Citrix ICA Clients support smart cards:
- ICA Client for Windows 32
- ICA Client for Linux
- ICA Client for Windows-based terminals

To configure smart card support for users of these clients, please see the *Administrator’s Guide* for the ICA Client or Clients in your environment.

**Interoperability with MetaFrame 1.8**

A single MetaFrame XP server farm can interoperate with a single MetaFrame 1.8 server farm when the MetaFrame XP farm is set to mixed mode. This mode provides limited pooling of connection license counts between MetaFrame 1.8 and MetaFrame XP servers, and allows applications to be published across MetaFrame 1.8 and MetaFrame XP servers.

**Important** For interoperability in mixed mode, Citrix recommends that you install the latest service pack on MetaFrame 1.8 servers. You can download service packs from Citrix at http://www.citrix.com/support/.

New features in feature releases for MetaFrame XP are not available when a server farm operates in mixed mode for interoperability with MetaFrame 1.8.

**Configuring MetaFrame XP for Mixed Mode Operation**

You can configure a MetaFrame XP server farm to operate in mixed mode when you install the first MetaFrame XP server in the farm. For information about configuring mixed mode during MetaFrame XP installation, see “Migrating to MetaFrame XP” on page 131.
After you install MetaFrame XP, you can configure the farm to operate in mixed mode using the Management Console for MetaFrame XP. For more information, refer to the console’s online help.

When you switch a MetaFrame XP server farm from mixed mode to *native mode*, (the mode in which only IMA-based servers participate in the server farm), the MetaFrame 1.8 and MetaFrame XP server farms become completely separate.

**Important** Make sure users cannot log on to the server farm if you need to change the interoperability mode.

Mixed mode is designed to facilitate migration to MetaFrame XP; it is not designed to be a permanent solution. After all MetaFrame 1.8 servers in the MetaFrame 1.8 farm are migrated to MetaFrame XP, be sure to set the MetaFrame XP server farm to operate in native mode using the Management Console.

The following issues and limitations affect operation in mixed mode:

**ICA Browser election.** In mixed mode, a MetaFrame XP server becomes the master ICA Browser on the subnet. On each MetaFrame XP server in the farm, the ICA Browser and Program Neighborhood-related services shut down and restart. During this process, ICA Clients might be unable to refresh applications in Program Neighborhood or browse for published applications, although current ICA connections are not affected. Therefore, it is best to switch to mixed mode when the fewest users need to connect to published applications.

**ICA license gateways.** In mixed mode, license gateways in the MetaFrame 1.8 server farm do not function for license pooling. You must set up license pooling across subnets using the Management Console for MetaFrame XP. For more information, see “Pooling License Counts in Mixed Mode,” below.

**Program Neighborhood service.** If you change the server farm from mixed mode to native mode before you migrate the entire MetaFrame 1.8 server farm to MetaFrame XP, you must stop and restart the Program Neighborhood service on all MetaFrame 1.8 servers that do not have MetaFrame 1.8 Service Pack 1 installed. If you do not restart the Program Neighborhood service, ICA Clients could have problems using published applications in the MetaFrame 1.8 server farm.

**Farm names.** The name you give to the MetaFrame XP server farm must be the same as the name of the MetaFrame 1.8 server farm. You enter the server farm name when you create the data store during MetaFrame XP installation on the first server in the farm.

**Subnet issues.** Do not use mixed mode if the server farm has no MetaFrame 1.8 servers operating in the same subnet as at least one MetaFrame XP server.
Active Directory and user logons. MetaFrame 1.8 servers do not support Active Directory. ICA Client users cannot enter user credentials in user principal name (UPN) format (user@domain) when a server farm operates in mixed mode. Entering UPN names can result in failure to display application sets and connect to published applications when clients connect to MetaFrame 1.8 servers.

Pooling License Counts in Mixed Mode

Pooling MetaFrame 1.8 connection license counts across subnets is not supported when you use mixed mode. When operating in native mode, MetaFrame XP combines connection license counts into a common pool for the entire server farm.

When operating in mixed mode, there is one pool of connection license counts for each IP subnet. Within each subnet, the pooled MetaFrame XP license counts and any pooled MetaFrame 1.8 license counts are combined and available to both MetaFrame 1.8 and MetaFrame XP servers. You can configure the percentage of connection license counts to allocate to each subnet on the Interoperability tab in the farm Properties dialog box in the Management Console for MetaFrame XP after mixed mode is enabled.

If you use license gateways to pool licenses between subnets, the gateways do not function when the server farm is interoperating with a new MetaFrame XP server farm in mixed mode.

Here is an example of how license gateways are affected by mixed mode:

There are two subnets, with four MetaFrame 1.8 servers on Subnet A and two MetaFrame 1.8 servers on Subnet B. Each server contributes 15 pooled licenses through a license gateway. If you run the Qlicense command on a MetaFrame 1.8 server, it displays 90 pooled licenses.

If you install a MetaFrame XP server on each subnet and add a 10-count connection license, each MetaFrame XP server becomes the master ICA Browser on the respective subnets; the license gateway stops functioning. The MetaFrame XP servers allocate the MetaFrame XP connection license counts to each subnet spanned by the MetaFrame XP farm but the MetaFrame 1.8 licenses are no longer pooled. By default, the MetaFrame XP connection licenses are allocated to each subnet evenly.

The connection license allocation percentages can be modified as described above. Using the default license allocation (which in this example is 50% for Subnet A and 50% for Subnet B), when you run Qlicense on the MetaFrame 1.8 servers on Subnet A, it reports 65 pooled licenses (4 MetaFrame 1.8 Servers * 15 licenses each + (50% * 10 MetaFrame XP license counts)).
When you run Qlicense on the MetaFrame 1.8 servers on Subnet B, it reports 35 pooled licenses (2 MetaFrame 1.8 servers * 15 licenses) + (50% * 10 MetaFrame XP license counts). The result is that the servers on Subnet A allow 65 concurrent connections while the servers on Subnet B allow 35 concurrent connections.

**Pooling MetaFrame for UNIX Licenses**

If your organization uses MetaFrame 1.8 for Windows and MetaFrame 1.0 or 1.1 for UNIX Operating Systems, you can pool connection licenses among the MetaFrame for Windows and MetaFrame for UNIX servers that are in the same subnet.

If you use IMA mixed mode to migrate the MetaFrame 1.8 for Windows servers to MetaFrame XP, connection license pooling continues between the MetaFrame 1.8 server farm and the MetaFrame for UNIX servers while the new MetaFrame XP server farm is in mixed mode for interoperability with MetaFrame 1.8.

When you complete the migration of MetaFrame 1.8 servers to MetaFrame XP and switch the new farm from mixed mode to native mode, the change causes license pooling with the MetaFrame for UNIX servers to stop. All licenses that were pooled in the MetaFrame 1.8 server farm move to the license pool of the new MetaFrame XP server farm.

Some organizations split licenses into two groups if their MetaFrame 1.8 for Windows and MetaFrame for UNIX servers are on different subnets. In this case, moving MetaFrame 1.8 servers to MetaFrame XP does not affect licensing because license pooling is not used with the MetaFrame for UNIX servers.

If you pooled license counts with MetaFrame for UNIX before migrating your MetaFrame 1.8 for Windows servers to MetaFrame XP, Citrix recommends that you configure your MetaFrame for UNIX servers in a separate subnet with sufficient connection license counts for the clients who connect to the servers. If you want to continue to pool license counts with MetaFrame for UNIX after migrating MetaFrame 1.8 servers to MetaFrame XP, contact your Citrix representative.

**Using MetaFrame XP Tools in Mixed Mode**

During MetaFrame XP installation, Setup installs all of the tools that are included with MetaFrame 1.8. All of the utilities work with both MetaFrame 1.8 and MetaFrame XP servers, with the exceptions described below.

**Citrix Server Administration.** This utility allows you to configure various options on MetaFrame XP servers. However, the settings take effect only when the server farm is operating in mixed mode.
Publishing applications. If you create or edit settings for published applications using the version of Published Application Manager included with MetaFrame XP, you cannot edit or delete the published applications using the version of Published Application Manager from MetaFrame 1.8. Use the version of the utility included with MetaFrame XP or installed with Service Pack 1 for MetaFrame 1.8.

MetaFrame XP does not support publishing videos using Citrix VideoFrame 1.0. Videos can still be launched from an ICA session using a .Cvi file.

Shadowing. In native mode, the Shadow Taskbar displays MetaFrame XP servers in a server farm. In mixed mode, the taskbar also displays MetaFrame 1.8 servers in the MetaFrame 1.8 server farm that is interoperating with the MetaFrame XP farm.

Client printer configuration. Use the Management Console for MetaFrame XP for all printer configuration and printer management for ICA Client users.
Installing MetaFrame XP

This chapter describes how to install and upgrade MetaFrame XP on Windows servers. Be sure to read “Planning for MetaFrame XP Deployment” on page 43 before you install MetaFrame XP.

If you are installing MetaFrame XP for the first time, installing MetaFrame XP from the MetaFrame XP CD-ROM also installs the latest feature releases and service packs. However, you must install and activate licenses for both MetaFrame XP and the latest feature release.

Creating the Data Store with SQL Server, Oracle, or DB2

To use Microsoft SQL Server, Oracle, or IBM DB2 for a server farm’s data store, use your database management software to create a database. Then, during MetaFrame XP Setup, configure each server’s ODBC driver to connect to the database. The following sections include the basic procedures for creating databases using Microsoft SQL Server, Oracle, or IBM DB2.

If you are setting up your farm to use Microsoft Access or the Microsoft SQL Server 2000 Desktop Engine (MSDE), you do not need to read this section and can skip to “Using the MetaFrame XP Windows Installer Package” on page 108. Using a Microsoft Access or MSDE database involves creating a database locally during the installation of MetaFrame XP on the first server in the farm.

To create a data store database with Microsoft SQL Server

Some dialog boxes might differ from the descriptions in this procedure, depending upon the version of Windows and SQL Server you use.

1. Run SQL Enterprise Manager on your Microsoft SQL server (Start > Programs > Microsoft SQL Server 7.0 > Enterprise Manager).
2. In the Enterprise Manager’s left pane, expand the tree until you reach the folder level.
3. Right-click the Databases folder and choose New Database.
4. A dialog box appears. In the **Name** box, enter a name and click **OK**.

5. Expand the Security folder.

6. Right-click **Logins** and choose **New Login**.

7. A dialog box appears with the **General** tab displayed. In the **Name** box, enter a name. Make note of the name because you will need to enter it during MetaFrame XP installation.

8. In the **Authentication** section of the **General** tab, click **SQL Server authentication** and enter a password. Remember the password; you must enter it during MetaFrame XP installation.

9. In the **Defaults** area of the **General** tab, change the **Database** to the name you specified in Step 4.

10. Click the **Database Access** tab. In the **Database** list, select the database name specified in Step 4.

11. In the **Database Roles** list, select **DB_Owner**. Leave other selected roles checked.

12. Click **OK**. You are prompted to confirm your password. Doing so completes database creation.

To create a data store database with Oracle

1. If you do not already have Oracle installed, install it using the default database.

2. On the Oracle server, run SQL Plus. At the connection prompt, type **internal**.

3. Use the following commands as guidelines for creating a tablespace and user:

   ```sql
   create tablespace MFXPIMA datafile 'D:\ORADATA\MFXPIMA.DBF' size 5000k autoextend on next 5000k maxsize unlimited;
   alter tablespace MFXPIMA default storage ( pctincrease 0 maxextents unlimited);
   create user MFXP identified by MFXP01 default tablespace MFXPIMA temporary tablespace TEMP;
   grant connect, resource to MFXP;
   ```

The tablespace is named MFXPIMA and saved in D:\ORADATA\MFXPIMA.DBF. The user is named MFXP and has the password MFXP01. Temp is the default temporary tablespace for Oracle8i. If you are using Oracle7, use TEMPORARY_DATA instead of TEMP.
To create a data store database with IBM DB2

1. If you do not already have an IBM DB2 database installed, install one using the default database.

2. Create a tablespace for MetaFrame XP using the following DB2 SQL script:

   ```sql
   CREATE REGULAR TABLESPACE CTXSDB PAGESIZE 4 K MANAGED
   BY SYSTEM USING ('C:\CTXSDB\XPFR3\') EXTENTSIZE 32
   OVERHEAD 8.3 PREFETCHSIZE 32 TRANSFERRATE 0.18
   BUFFERPOOL IBMDEFAULTBP
   COMMENT ON TABLESPACE CTXSDB IS '');
   ```

3. Create a local user account called “XPFR3ADMIN” and then use the following DB2 SQL script to grant this account use of the tablespace:

   ```sql
   GRANT USE OF TABLESPACE CTXSDB TO USER XPFR3ADMIN WITH
   GRANT OPTION
   GRANT USE OF TABLESPACE CTXSDB TO PUBLIC WITH GRANT
   OPTION
   ```

   In the example above, the tablespace is named CTXSDB and saved in C:\CTXSDB\XPFR3\sqltag.nam. The user is named XPFR3ADMIN.

### Changing Server Drive Letters

When a user launches an ICA session, a MetaFrame XP server attempts to map disk drives on the server to the typical drive letters for the client. If the drive letters are available, the server maps the client’s first floppy disk drive to A, the second floppy drive to B, the first hard disk drive to C, and so on. However, a server cannot map client device drives to letters that are assigned to the server’s own disk drives.

By changing the server to use drive letters that are higher, such as M, N, or O, the original lower drive letters become available for assignment to the drives on client devices. This can make the use of drives on client devices less confusing for users, because they see their drives identified by typical drive letters.

If you want to change server drive letters, Citrix recommends that you do so before installing MetaFrame XP and before installing applications on the MetaFrame XP server. Changing server drive letters after MetaFrame XP installation can cause unstable performance by the server, components of the operating system, and installed applications.

If you are installing MetaFrame XP for the first time on a clean system, you can change the server’s drive letters by selecting **Install or update MetaFrame** from the MetaFrame XP Setup Autorun screen. Alternatively, you can run DriveRemap.exe, located on the MetaFrame XP server CD. For more information about the **DriveRemap** utility, see “DRIVEREMAP” on page 338.
CAUTION With utilities provided in Windows, it is possible to change server drive letters after MetaFrame XP installation. Citrix advises against changing server drive letters after MetaFrame XP installation. Doing so can destroy data stored on disk drives and can leave MetaFrame XP and the operating system unable to operate.

**Using the MetaFrame XP Windows Installer Package**

MetaFrame XP Setup is compiled into a Windows Installer installation package. Windows Installer is a component of the Windows operating system that manages the installation and removal of applications. Windows Installer applies a set of centrally defined setup rules during the installation process that define the configuration of the application.

Windows Installer technology consists of the Windows Installer Service for the Windows operating systems and the package (.msi) file format used to hold information regarding the application setup. You use the Windows Installer Service to modify, repair, or remove an existing application that was installed using Windows Installer technology. Go to **Add/Remove Programs** in Control Panel to remove or modify Windows Installer packages installed on the system.

You can deploy Windows Installer packages using Installation Manager or Microsoft Active Directory Services or Systems Management Server. For more information about Windows Installer technology and the Windows Installer Service, see the Windows online Help or the Microsoft Web site at http://www.microsoft.com.

For more information about working with the MetaFrame XP Windows Installer installation package, see “Customizing MetaFrame Setup” on page 367.

If you encounter problems when running a Windows Installer package, you can check the Windows Event Viewer for a list of the problems. To open Event Viewer, go to **Start > Program Files > Administrative Tools > Event Viewer**. Check the Application Log for any entries in the Source column of the type “MSIInstaller.”

**Common Windows Installer Commands**

You can use the Msiexec command to install, modify, and perform operations on Windows Installer packages from the command line. The MetaFrame XP Windows Installer package, named MFXP001.msi, is located on the MetaFrame XP CD-ROM in the directory `\MetaFrame\<Platform>`, where *Platform* is the operating system on which you plan to run MetaFrame XP.
You also use the Msiexec command to run administrative installations. Administrative installations allow you to store preconfigured, customized images of MetaFrame XP Setup on network share points. You can then access the MetaFrame XP Windows Installer installation package and install MetaFrame XP from anywhere on your network. For more information about creating customized administrative installation share points, see “Customizing MetaFrame Setup” on page 367.

Some common options for the Msiexec command are listed below. For further information about the parameters and switches you can use with the listed options, go to the Microsoft Web site and search on “msiexec.”

<table>
<thead>
<tr>
<th>Option</th>
<th>Syntax</th>
</tr>
</thead>
<tbody>
<tr>
<td>Install or configure a product</td>
<td>msiexec /i {package</td>
</tr>
<tr>
<td>Uninstall a product</td>
<td>msiexec /x {package</td>
</tr>
<tr>
<td>Set a logging level</td>
<td>msiexec /L [i][w</td>
</tr>
<tr>
<td>Set the user interface level</td>
<td>msiexec /q {n</td>
</tr>
</tbody>
</table>

### Creating a Log File

Installation and uninstallation log files are not automatically created for Windows Installer packages in Windows. You can create log files with the following methods:

- Use the logging command to create log files for only the Windows Installer operation you are carrying out.

- Turn on automatic logging for all Windows Installer operations by creating a new registry string value at.

  Key: HKLM\SOFTWARE\Policies\Microsoft\Windows\Installer

  String (REG_SZ) Value: Logging

  Contents: iwearucmopv

  A log file is created in the %Tmp% directory for each operation.
• Use Active Directory’s Group Policy Editor to configure logging properties for an Active Directory group.

To edit the Logging policy, open Group Policy Editor and select **Computer Configuration > Administrative Templates > Windows Components > Windows Installer.**

### Unattended Setup of MetaFrame XP Servers

You can configure MetaFrame XP Setup to run without assistance with the following methods:

• Applying transforms to the installation database. A Windows Installer transform modifies the installation package file at installation time and applies the values you set. Sample transform files are located on the MetaFrame XP CD-ROM at Support\Install.

• Creating an answer file to provide answers to the questions asked during Setup. A sample answer file is located on the MetaFrame XP CD-ROM at Support\Install.

The following sections describe creating and applying transforms and creating answer files.

### Applying Transforms

You can manipulate the installation process by applying Windows Installer transforms (files with the .mst extension) to the installation database contained in a Windows Installer package. A transform makes changes to elements of the database. A transform file modifies the installation package when it is being installed and dynamically affects the installation behavior.

When you create a transform to apply to the MetaFrame XP Windows Installer package, you set your desired values for properties in the package. When you then apply the transform to the installation package, the “questions” you would be asked during Setup are answered. Creating a transform allows you to roll out MetaFrame XP in unattended mode.

Transforms that you create to customize a Windows Installer setup package remain cached on your system. These files are applied to the base Windows Installer package whenever the Installer needs to modify it. You can apply transforms only when you initially install Windows Installer packages; you cannot apply transforms to software that is already installed.
Citrix provides four sample transforms on the MetaFrame XP CD-ROM. You can open these transforms and edit the properties in them using commercially available Windows Installer editing tools. The sample transforms include sample values for select properties, allowing you to determine which properties to edit to achieve a certain configuration.

For more information about each sample transform and the properties you can set for each configuration, see “Customizing MetaFrame Setup” on page 367.

To create a customized transform using one of the sample transform files
1. Using your preferred tool for editing Windows Installer packages, open the MetaFrame XP Setup Windows Installer installation package, MFXP001.msi, located on the MetaFrame XP CD in the \MetaFrame directory.
2. Apply the transform that includes the properties and values you want to modify.
3. Enter new values for the properties you want to change.
4. Generate the transform file.
5. Save the file with a new name.

Creating an Answer File

You can create an answer file to provide answers to the questions asked when you run MetaFrame XP Setup. A sample answer file is located on the MetaFrame XP CD-ROM at Support\Install. Instructions are provided in the file for setup options. Copy the sample answer file to another location and modify it for your needs.

To perform an unattended installation
1. Insert the MetaFrame XP CD-ROM in the CD-ROM drive of the server, or insert the MetaFrame XP CD-ROM in a CD-ROM drive accessible over the network. If your CD-ROM drive supports Autorun, the MetaFrame XP CD-ROM splash screen appears. Close the window.
2. Open the sample file XPFR3_UnattendedTemplate.txt, located in the directory Support\Install, in any text editor. Save the file with another name.
3. Enter the values for the entries you want to set. The sample file includes definitions and possible values for each entry.
4. Type the following at a command prompt where <Windows Installer package> is the name of the Windows Installer package you want to run, and <answer file> is the name of the text file you created in Step 2:

   UnattendedInstall <Windows Installer package> <answer file>
Starting MetaFrame XP Setup

Insert the MetaFrame XP CD-ROM in the CD-ROM drive. If your CD-ROM drive supports Autorun, the MetaFrame XP splash screen appears. Selected Autorun installation options are described below.

View installation checklist. Read this document for important recommendations from Citrix.

Install or update MetaFrame. Click to access options to install or upgrade MetaFrame XP with the latest feature release or service pack.

Other tools and components. Click to access options to install MetaFrame XP management tools, including the Management Console for MetaFrame XP, the Web Console, and Network Manager Components.

Browse. This option displays the contents of the CD.

The following procedures explain how to install MetaFrame XP using the MetaFrame XP CD-ROM. For more information, including descriptions of Setup options, see “Choosing Options During Setup” on page 113.

CAUTION Your Windows server must be running Windows Installer Version 2.0 or later before you install MetaFrame XP. MetaFrame XP Setup exits if it does not detect an updated version of Windows Installer on the server. You can download the latest version of Windows Installer from the Microsoft Web site at http://www.microsoft.com. Version 2.0 of Windows Installer is included on the MetaFrame XP CD in the directory \Support\MSI20.

To begin MetaFrame XP Setup

1. Exit all applications.
2. Insert the MetaFrame XP CD-ROM in the CD-ROM drive. If your CD-ROM drive supports Autorun, the MetaFrame XP splash screen appears.
3. Click View installation checklist for important recommendations from Citrix.
4. Click Install or update MetaFrame to install MetaFrame XP with the latest feature release or service pack. If you are installing MetaFrame XP for the first time on a clean system, click this button.
5. Click MetaFrame XP Service Pack X to install MetaFrame XP and the latest MetaFrame XP service pack. Click MetaFrame XP Feature Release X to install MetaFrame XP and the latest feature release.
Chapter 4  Installing MetaFrame XP  113

**Note**  Selecting the **MetaFrame XP Feature Release X** option installs the latest feature release and service pack. Features included in the latest feature release require additional licensing.

If you are installing MetaFrame XP on a clean system, selecting the **MetaFrame XP Feature Release X** option installs all newly released and previously released feature releases and service packs.

When MetaFrame XP Setup begins, a series of information pages and dialog boxes ask you to select options and configure MetaFrame XP. Click **Next** to continue after you complete each entry. If you want to return to a previous page to make changes, click **Back**. If you click **Cancel**, Setup stops without finishing.

**Using the Command Line**

You can also use the Msiexec command to install MetaFrame XP. Set properties by adding `<Property="value">` on the command line after other switches and parameters. For definitions of the properties in the MetaFrame XP Windows Installer package, see “Customizing MetaFrame Setup” on page 367.

The following sample command line installs the MetaFrame XP Windows Installer package and creates a log file to capture information about this operation. Add the properties you want to set after the switches.

```
msiexec /i MFXP001.msi /L*v c:\output.log
```

**Choosing Options During Setup**

The following sections describe the various aspects of MetaFrame XP configuration that you perform during MetaFrame XP Setup.

**Selecting the MetaFrame XP Family Level**

Select the family level you are licensed to run on the MetaFrame XP server. When you purchase MetaFrame XP, you can select from three family levels:

- **MetaFrame XPe** is designed for single-point control of servers, licenses, and resources in large organizations and multinational corporations. A MetaFrame XPe license enables all of the features of MetaFrame XPa and also provides system monitoring and analysis, application packaging and delivery, and integration with third-party SNMP management consoles.

- **MetaFrame XPa** is designed with the small to medium business in mind. A MetaFrame XPa license enables all of the features of MetaFrame XPs and also includes load balancing functionality.
MetaFrame XPs is designed to give businesses outstanding performance from applications running on a central server.

If you have questions about which family level to choose, contact your MetaFrame XP reseller or go to the Product Information area of the Citrix Web site at http://www.citrix.com/products.

Based on which family level you are installing, Setup selects the components to install.

**Choosing the Product Type**

Select the MetaFrame XP product type you are installing. When you select a product type, the MetaFrame XP product code is automatically set. Be sure to verify that the correct product code is displayed on the Setup screen. You can find the product code on the MetaFrame XP media pack.

If you need to enter the product code manually, select Other on the Setup screen and then enter the correct product code.

For more information about licenses and product codes, see “Licensing MetaFrame XP” on page 137.

**Selecting Components**

Based on which family level of MetaFrame XP you are installing (MetaFrame XPs, MetaFrame XPa, or MetaFrame XPe), Setup selects the components to install.

The components to be installed are displayed on the Component Selection Setup screen. Click Disk Cost to check the amount of disk space the selected components require.

**Installing the ICA Pass-Through Client**

You can install an ICA Pass-Through Client on the MetaFrame XP server. When you install the Pass-Through Client, you can:

- Allow users to run the ICA Win32 Client on the MetaFrame XP server to access published resources
- Test client-to-server connectivity in your MetaFrame XP server farm

When you install a Pass-Through Client, you are prompted later during Setup to configure Pass-Through Authentication. Pass-Through Authentication allows the user’s local credentials to be passed to the MetaFrame XP server for authentication.

You can install the full ICA Win32 Program Neighborhood Client or the Program Neighborhood Agent. The full Program Neighborhood Client is selected by default.
If you want to install the Program Neighborhood Agent, click the Program Neighborhood Agent component and select **Will be installed on local hard drive**.

If you install the Program Neighborhood Agent, you are prompted later during Setup to enter the URL of the server running the Web Interface for MetaFrame XP. This server hosts the Program Neighborhood Agent configuration file. By default, MetaFrame XP attempts to resolve “localhost” and enters the results of the resolution.

**Installing WMI Providers**

MetaFrame XPe includes support for the management technology that integrates the monitoring of Citrix MetaFrame XPe servers and server farms into Microsoft Operations Manager (MOM) 2000, the latest network and server management tool from Microsoft.

Windows Management Instrumentation (WMI) is the standard management infrastructure included as part of Microsoft Windows 2000 and Windows XP. The WMI Provider for MetaFrame XP supplies the information about MetaFrame XPe servers and server farms that is displayed in the MetaFrame XP Management Pack for MOM.

You must install the WMI Provider on each MetaFrame XP server you want to monitor with MOM.

The MetaFrame XP Management Pack for MOM, in conjunction with the WMI Provider, allows you to monitor the health and performance of MetaFrame XP servers and underlying Microsoft Windows servers using the MOM environment.

The MetaFrame XP Management Pack is a plug-in for MOM that you can use to monitor the health and availability of MetaFrame XPe servers and server farms. MOM provides real-time event and performance monitoring and includes an extensive knowledge base, with links to Citrix Knowledge Base articles and other sources of information.

**Creating a New MetaFrame XP Server Farm**

When you run MetaFrame XP Setup on the first server in a server farm, you create a MetaFrame XP server farm. Before you create a new server farm, you must decide the following things:

- What database to use to host the server farm’s data store. If you are using Microsoft Access or Microsoft SQL Server 2000 Desktop Engine (MSDE), the database is created on the first MetaFrame XP server on which you run Setup.
- What to name the new MetaFrame XP server farm.
- Which user account should be initially granted full access to all server farm management tasks.
For more information about and recommendations for these issues, see “Planning for MetaFrame XP Deployment” on page 43.

**Joining an Existing MetaFrame XP Server Farm**

When you want to add more servers to a server farm, you run MetaFrame XP Setup on the servers and join the existing farm. When you join an existing server farm, you must have the following information at hand:

- If you are using a database stored on the first server in the farm (Microsoft Access or MSDE), you need the name of that server and the logon credentials of a user authorized to access the database.
- If you are using a third-party database stored on a separate, dedicated server (Microsoft SQL Server, Oracle, or IBM DB2), you need to know which type of database is configured to host the data store. You must also have the logon credentials of a user authorized to access the database.

**Configuring the Data Store**

This section explains how to configure MetaFrame XP servers to connect to the data store for a server farm. For background information about the data store, see “Choosing a Database for the Data Store” on page 50. For background information about server farm zones, see “Configuring Zones and Data Collectors” on page 189.

**Using Microsoft Access or MSDE for the Data Store**

To use a Microsoft Access or SQL Server 2000 Desktop Engine (MSDE) database for a server farm data store, you create the database when you install MetaFrame XP on the first server in the farm. Additional servers connect to the first server using TCP port 2512. If you want to use another port, use the IMAPORT command to change the port on the first server. For more information about this command, see “MetaFrame XP Commands” on page 311. You can specify the port number for the other servers during MetaFrame XP installation.

- **To create a server farm using Access or MSDE for the data store**
  1. On the Create or Join a Server Farm Setup screen, select **Create a new farm** and click Next.
  2. On the Create a Server Farm Setup screen, enter the following information:
     - Enter a name for the new MetaFrame XP server farm. Farm names can include spaces but cannot be more than 32 characters in length.
     - Select **Use a local database on this server** and then choose from Access Database or SQL Server Desktop (MSDE) Database.
Important  If you want to use SQL Server Desktop (MSDE) for your MetaFrame XP server farm’s data store, you must install MSDE on the MetaFrame XP server before you run MetaFrame XP Setup. For more information about installing MSDE, see “Microsoft SQL Server 2000 Desktop Engine (MSDE)” on page 56.

- The default zone name is the mask for the subnet in which the server resides. If you want to change the server farm zone name, clear the option Use Default Zone Name and enter the new name.

3. Click Next to continue.
4. Continue with MetaFrame XP Setup.

To add more servers to the server farm
1. On the Create or Join a Server Farm Setup screen, select Join an existing farm and click Next.

2. Select Connect to a database on this MetaFrame XP server, and then enter the name of the MetaFrame server hosting the Access or MSDE database. The default communication port is 2512.

3. Accept the default zone name or enter a different zone name.
4. Continue with MetaFrame XP installation.

Using SQL, Oracle, or IBM DB2 for the Data Store
The following procedure describes options that appear during MetaFrame XP Setup as part of the MetaFrame XP installation. The same procedures are used whether the data store is a Microsoft SQL database, an Oracle database, or an IBM DB2 database.

Before starting MetaFrame XP Setup, you must create the data store database using your database management software; see the procedures “To create a data store database with Microsoft SQL Server” on page 105, “To create a data store database with Oracle” on page 106, or “To create a data store database with IBM DB2” on page 107.

To create a server farm with a SQL, Oracle, or DB2 data store
Follow this procedure only on the first server in the farm on which you install MetaFrame XP. See the next procedure for configuring the remaining servers in the farm.

1. On the Create or Join a Server Farm Setup screen, select Create a new farm and click Next.
2. On the **Create a Server Farm** Setup screen, enter the following information:
   - Enter a name for the new MetaFrame XP server farm. Farm names can include spaces but cannot be more than 32 characters in length.
   - Select **Use the following database on a separate database server** and select the database from the list.
   - The default zone name is the mask for the subnet in which the server resides. If you want to change the server farm zone name, clear the option **Use Default Zone Name** and enter the new name.

3. Click **Next** to continue.

4. Continue with MetaFrame XP Setup.

5. Follow the procedure “To configure the ODBC driver for Microsoft SQL Server” on page 118, “To configure the ODBC driver for Oracle” on page 121, or “To configure the ODBC driver for IBM DB2” on page 122.

6. Follow the remaining instructions in Setup.

   This completes data store configuration of the first server in the farm.

   **To add more servers to the server farm**
   1. On the **Create or Join a Server Farm** Setup screen, select **Join an existing farm** and click **Next**.

   2. Select **Connect directly to the database using ODBC**. Select your database from the list and then click **Next**.

   3. Follow the instructions in the procedure “To create a server farm with a SQL, Oracle, or DB2 data store” beginning with Step 3.

   **Configuring ODBC Drivers**

   This section provides step-by-step instructions for configuring ODBC drivers for Microsoft SQL Server, Oracle, and IBM DB2 databases. Some of the dialog boxes shown are components of Microsoft’s ODBC manager and may differ from those you see, depending upon the version of Windows and the ODBC driver you are using.

   **To configure the ODBC driver for Microsoft SQL Server**

   1. When you select your SQL driver from the database list in MetaFrame XP Setup, the following dialog box appears:
Leave the **Name** field as is. Click the pull-down list next to the **Server** field and select your SQL Server machine in the list. Click **Next**.

2. The following dialog box appears:

This dialog box lets you specify the method of authenticating the logon ID that MetaFrame XP will present to the SQL Server when accessing the data store. To authenticate successfully, the SQL Server and MetaFrame XP must use the same authentication method. Make sure the database created for MetaFrame XP by the database administrator is using SQL Server authentication.

Choose **With SQL Server authentication**. In the **Login ID** field, specify the logon created by the database administrator. In the **Password** field, specify the password for the Logon ID. Click **Next**.

If the ODBC manager is unable to authenticate to the database, you are prompted to reenter the Logon ID and password.
3. The following dialog box appears:

![Create a New Data Source to SQL Server dialog box]

Click **Change the default database to** and select the name of the database you created for MetaFrame XP if it is not already selected.

**Note** SQL Server logon IDs can be configured to log on to a database by default. If in your SQL Server administrative program the logon ID is set to log on to the data store database by default, you do not have to specify a default database in this dialog box.

4. Click **Next**. The following dialog box appears:

![Create a New Data Source to SQL Server dialog box]

Click **Finish** to accept these values. A dialog box lets you test the new data source name. Click **Test Data Source**. If the test completes successfully, click **OK** and then click **OK** again to complete data source name configuration.
5. Follow the steps in the procedure, “To create a server farm with a SQL, Oracle, or DB2 data store” on page 117, beginning with Step 6.

- **To configure the ODBC driver for Oracle**
  1. If you select an Oracle driver from the database list in MetaFrame XP Setup, the following dialog box appears:

![Oracle ODBC Driver Connect dialog box]

  2. In the **Service Name** box, type the service name used when the Oracle client was installed. In the **User Name** and **Password** boxes, type the user name and password created on the Oracle server for the data store.

  3. Click **OK**.

This completes the Oracle data store setup. You are now ready to install MetaFrame XP. Follow the steps in the procedure “To create a server farm with a SQL, Oracle, or DB2 data store” on page 117, beginning with Step 6.
To configure the ODBC driver for IBM DB2

1. If you select “IBM DB2 ODBC DRIVER” from the database list in MetaFrame XP Setup, the following dialog box appears:

2. Set the connection mode to Share.

3. Click Add to launch the IBM DB2 Client Configuration Assistant. This wizard walks you through configuring the ODBC connection to the DB2 database.

4. Follow the instructions in the Client Configuration Assistant. On the Protocol page, be sure TCP/IP is selected. Citrix recommends that you use this protocol to connect to the data store.

5. Click Finish when you are done configuring the connection.

6. On a Windows Server 2003 server, Click Test Connection to make sure that the connection to the database works.

7. Click Close.

8. Ensure that the connection mode is still set to Share.

9. Enter the User ID and Password.

10. Click OK.

This completes the DB2 data store setup. You are now ready to continue with MetaFrame XP Setup. Follow the steps in the procedure “To create a server farm with a SQL, Oracle, or DB2 data store” on page 117, beginning with Step 6.
Assigning Farm Administrator Credentials

MetaFrame XP administrators manage MetaFrame XP server farms. When you install the first MetaFrame XP server in a new server farm, you specify an initial farm administrator. This user account is automatically configured as a MetaFrame XP administrator with full administration rights to all farm management tasks in the Management Console for MetaFrame XP.

To give other user accounts access to the console, a MetaFrame XP administrator with full administration rights logs on to the console and creates other MetaFrame XP administrator accounts.

You can create MetaFrame XP administrator accounts with the following permission levels:

- Full administration rights to all areas of MetaFrame XP server farm management.
- View-only access to all areas of server farm management.
- Access to areas of farm management or specific tasks within those areas; administrators can have a mixture of view-only access, write access, or no access.

For more information about delegating administration rights to MetaFrame XP administrators, see “Configuring MetaFrame XP Administrator Accounts” on page 174.

**Note** One MetaFrame XP administrator account with full administration rights must always exist in the server farm. MetaFrame XP prevents you from deleting the last MetaFrame XP administrator account with this level of permission. However, if the account no longer exists in the network account authority, the console allows a local administrator to log on to the console to set up MetaFrame XP administrator accounts.

Configuring Session Shadowing

You use MetaFrame XP’s *session shadowing* to monitor and interact with users’ ICA sessions. When you shadow an ICA session, you can view everything that appears on the session display. You can also use remote control features to control the mouse and enter keystrokes from a remote location.

Shadowing can be a useful tool for user collaboration, training, troubleshooting, and monitoring by supervisors, help desk personnel, and teachers.
During MetaFrame XP installation, you can limit or disable shadowing. You can disable shadowing of ICA sessions on all servers in your server farm if legal privacy requirements prohibit shadowing of users’ sessions. Alternatively, you may want to disable shadowing on servers that host sensitive applications, such as personnel or payroll applications, to protect confidential data. MetaFrame XP Setup provides options on the Configure shadowing Setup page for you to limit or disable shadowing.

**Important** Shadowing restrictions are permanent. If you disable shadowing, or enable shadowing but disable certain shadowing features when you run MetaFrame XP Setup, the restrictions cannot be changed at a later time. If you place restrictions on shadowing during Setup, any user policies you create to enable user-to-user shadowing have no effect.

Do not disable shadowing as a substitute for instituting user- and group-specific permissions for ICA connections. Disabling shadowing for ICA sessions does not affect RDP sessions. Use Terminal Server Connection Configuration to disable shadowing of RDP sessions or remove the RDP connections completely.

**Prohibit shadowing of ICA sessions on this server.** This option permanently disables shadowing by anyone of all ICA sessions on the server. If you disable shadowing during MetaFrame XP Setup, you cannot allow shadowing using other MetaFrame XP configuration utilities or by creating user policies.

**Allow shadowing of ICA sessions on this server.** This option enables shadowing of ICA sessions hosted by the server. When you enable shadowing, you have the option to select the following restrictions:

- **Prohibit remote control.** By default, MetaFrame XP gives users with permission to shadow the ability to input keystroke and mouse control during session shadowing. Select this option if you want these users to be able to shadow without input. In some cases, shadowing without input hides the user’s presence.

- **Force a shadow acceptance popup.** By default, MetaFrame XP notifies users with a prompt when other users are attempting to shadow their sessions. Select this option to deny users the ability to shadow sessions without sending this notification.

- **Log all shadow connections.** Events such as shadowing attempts, successes, and failures can be logged in the Windows event log and examined using Event Viewer. Select this option to enable logging.
Configuring Network ICA Connections

By default, MetaFrame XP Setup enables ICA connections over the TCP/IP network protocol only.

If you want to enable ICA connections over a different network protocol, install the protocol under Windows networking and then use the Citrix Connection Configuration utility to enable ICA connections for the newly-installed protocol.

Note Windows Server 2003 supports only the TCP/IP protocol for remote connections.

Installing the Web Interface for MetaFrame XP

The Web Interface is a component of MetaFrame XP that you can use to provide users with access to MetaFrame XP applications through a standard Web browser. When you install MetaFrame XP, the Web Interface is also installed if the server is running Microsoft Internet Information Services Version 5.0 or later.

The Web Interface employs Java object technology executed on a Web server to dynamically create an HTML-based depiction of the MetaFrame XP server farm for each of your users. Included in each user's presentation are all the applications published in the MetaFrame XP server farm for that user.

For large-scale deployments, Citrix recommends that you run the Web Interface on dedicated Web servers. For smaller deployments, you can run Web server software and the Web Interface together on a MetaFrame XP server.

For more information about configuring the Web Interface for MetaFrame XP, see the Web Interface Administrator’s Guide, located in the Docs directory of the MetaFrame XP Server CD-ROM.

Configuring the Citrix XML Service Port

MetaFrame XP uses the Citrix XML Service to supply servers running the Web Interface for MetaFrame XP and ICA Clients with the names of applications published on MetaFrame XP servers. By default, MetaFrame XP Setup configures the Citrix XML Service to share the default TCP/IP communication port (port 80) with Microsoft Internet Information Services.

If you intend to send data to the Web Interface for MetaFrame XP over a secure HTTP connection using SSL, be sure that the Citrix XML Service is set to share its port with IIS and that IIS is configured to support HTTPS.
If you do not want the Citrix XML Service to share the TCP port with IIS, you can use a separate port for the Citrix XML Service. On the Configure Citrix XML Service Port Setup page, select Use a separate port and enter the new port number. If you plan to change the port used by the Citrix XML Service on MetaFrame XP servers, make sure the port you plan to use is not used by any other application.

For a list of ports in use, type `netstat -a` at a command prompt. Make a note of the port number you specify. If you use a port other than the default port 80, you must configure servers running the Web Interface and any ICA Clients using TCP/IP + HTTP server location to use the port you choose. See the Web Interface for MetaFrame XP Administrator's Guide for instructions about configuring the Web Interface for MetaFrame XP to use a different port. See the ICA Client Administrator's Guides for instructions about configuring the ICA Clients to use a different port.

**Important** All of the MetaFrame XP servers in the server farm must use the same TCP port for the Citrix XML Service. This requirement includes all MetaFrame 1.8 and MetaFrame XP servers when operating in mixed mode.

### To change the Citrix XML Service port after installation

**Important** Use this procedure only if you do not want to share the port used by Internet Information Services. If you entered a port number other than the default “Share with IIS” during MetaFrame XP Setup, you can change the port to another port number using the Management Console for MetaFrame XP. However, if you want to change the setting to share the port with IIS after running MetaFrame XP Setup, you must follow the instructions for manually setting the Citrix XML Service to share the TCP port with IIS.

1. Use the Services icon in the Control Panel to stop the Citrix XML Service. On Windows 2000 servers, this icon is in the Administrative Tools folder in the Control Panel folder.
2. At a command prompt, type `ctxxmlss /u` to unload the Citrix XML Service from memory.
3. Type `ctxxmlss /rnn`, where `nn` is the number of the port you want to use. For example, `ctxxmlss /r88` forces the Citrix XML Service to use TCP/IP port 88.
4. Restart the Citrix XML Service in the Control Panel.
To manually configure Citrix XML Service to share the TCP port with Internet Information Service

1. Use the Services Control Panel to stop Citrix XML Service. On Windows 2000 servers, this icon is in the Administrative Tools folder in the Control Panel folder.

2. At a command prompt, type `ctxxmlss /u` to unload the Citrix XML Service.

3. Copy Wpnbr.dll and Ctxxmlss.txt to the IIS scripts directory on your Web server. These files are installed to `%SystemRoot%\System32\` during MetaFrame XP installation. The default scripts directory is `%RootDrive%\inetpub\scripts`.

4. Use Internet Service Manager to give the files read and write access.

5. Stop and restart the Web server.

Setting the Server’s Default Web Page

By default, MetaFrame XP Setup sets the server’s default Web page to the login page for the Web Interface. Users can access this login page by pointing their Web browsers to `http://<server name>`, where `<server name>` is the name of the MetaFrame XP server running the Web Interface.

If you do not want to set the MetaFrame XP server’s default Web page to the login page for the Web Interface, be sure this option is not selected.

Installing ICA Client Software

At the end of MetaFrame XP Setup, you can run the ICA Client Distribution wizard to install ICA Clients and ICA Client-related utilities. Use the MetaFrame XP Components CD to access the initialization file needed to run this wizard. For more information about deploying and configuring ICA Clients, see “Deploying ICA Clients to Users” on page 219.

Create or update ICA Client images. The ICA Client Creator is a MetaFrame XP server utility you use to create installation disks for Windows and DOS ICA Clients. The ICA Client Distribution wizard places copies of ICA Clients in the database from which this utility creates client disks.

Note The ICA Client Creator utility is not supported on Windows Server 2003.
Create or update the ICA Client Update Database. Client Auto Update is a feature that enables you to schedule the download and installation of the latest ICA Client software from MetaFrame XP servers to client devices. The ICA Client Distribution wizard places copies of ICA Clients in the database on the MetaFrame XP server used by Client Auto Update.

Install or upgrade the ICA pass-through Client on the server. MetaFrame XP servers can include an installed copy of the ICA Win32 Client. You can publish the server’s desktop to allow users to access the Program Neighborhood interface. The ICA Client Distribution wizard installs the ICA Win32 Program Neighborhood Client on the MetaFrame XP server.

Install ICA Client Administrator’s Guides. The wizard can copy the ICA Client Administrator’s Guides in PDF format to the Program Files\Citrix\Documentation directory on the server.

When the wizard prompts you to specify the location of your ICA Client CD-ROM, insert the MetaFrame XP Components CD in the server’s CD-ROM drive and click Next. Alternatively, you can specify the location of a network-shared Components CD-ROM or CD image. The wizard requires you to type in or browse to the location of the file ICASetup.ini. This file is located in the root directory of the Components CD.

The wizard includes typical and custom installation paths. A typical installation does the following:

- Installs the Client Auto Update Database and copies each ICA Client into the database
- Installs the ICA Client Creator database and copies each ICA Client into the database
- Installs the ICA Win32 Client on the server
- Copies the ICA Client Administrator’s Guides to the %SystemDrive%\Program Files\Citrix\Documentation\ICA Clients directory on the server

When performing a custom installation, a dialog box gives you options for installing ICA Clients and documentation.

If you select Create/Update Citrix ICA Client Images or Create/Update Citrix ICA Client Update Database, dialog boxes let you select ICA Clients to install. For example, if you choose to Create/Update Citrix ICA Client Images, a dialog box lets you select ICA Clients to add to the ICA Client Creator’s database. Clear the check boxes for ICA Clients you do not want to add to the database.
Upgrading to MetaFrame XP Feature Releases

Citrix recommends that you deploy the latest feature release and service pack in all server farms. The feature release updates your MetaFrame XP software to the latest version.

**Note**  If you find that you need to run different releases of MetaFrame XP in your server farm on a temporary basis, configure a server running the latest release as the zone’s data collector. See “Configuring Zones and Data Collectors” on page 189 for more information.

When you install the most recently released service pack, all previously released service packs are also installed; you do not need to install each service pack separately. However, if you do not want to install the latest feature release, you can install the latest service pack to apply its fixes for known issues and performance improvements in your MetaFrame XP server farm.

If you do not have MetaFrame XP installed, running MetaFrame XP Setup installs the latest feature release and service pack and does the following:

- Installs new features and provides enhancements to existing features. Installing the latest feature release adds the enhancements and new features to the server’s application server software, the Management Console for MetaFrame XP, and the additional components that are part of MetaFrame XPa and MetaFrame XPe.

- Provides performance improvements and fixes known issues. Installing the latest service pack on a MetaFrame XP server updates the application server software, the Management Console for MetaFrame XP, and the additional components that are part of MetaFrame XPa and MetaFrame XPe.

For a summary of new features and improvements that are provided by Feature Release 3, see “Features Included in Feature Release 3” on page 26.

**Important**  If you are upgrading MetaFrame servers that have a previous release of Resource Manager installed, upgrade the farm metric servers (primary and backup) before upgrading other MetaFrame servers in the server farm. Resource Manager uses the farm metric server to interpret information collected from other servers. This may cause inconsistencies if another server is running a later version of Resource Manager.
Downgrading to a Previous MetaFrame XP Feature Release

You can downgrade a service pack or feature release if necessary. Downgrading the software returns the MetaFrame XP server to its state before the feature release or service pack was installed.

- **To downgrade to an earlier version of MetaFrame XP**
  1. Choose **Start > Settings > Control Panel > Add/Remove Programs**.
  2. Select the service pack or feature release from the list of installed programs.
  3. Click **Change**. Do not click **Remove**. Doing so uninstalls MetaFrame XP from your system.
  4. On the **Application Maintenance** screen, click **Remove** and then click **Next**.
  5. On the **Citrix MetaFrame XP for Windows, Feature Release X Uninstall** screen, click **Downgrade**.

Setting a Server’s Feature Release Level

The feature release level is a setting that enables a feature release on a MetaFrame XP server. Normally, the feature release level is set when you install and license a MetaFrame XP feature release. You can set the feature release level manually to change a server’s configuration.

For example, you can set the feature release level to an updated feature release if you installed a service pack only (which does not set the feature release level), and now you want to enable the feature release software.

The feature release level affects the product license that the server requires. The following are examples of the effect of the feature release setting:

- If a server’s feature release level is set to Feature Release X, the server seeks a Feature Release X product license from the server farm’s license pool. If the license is available, the feature release software is enabled and its features are available on the server. If the Feature Release X license is not available, the server does not accept connections from ICA Clients.
- If a server’s feature release level is set to “Not Installed,” the server does not seek a feature release product license and the features of the feature release are not available on the server.

- **To set the feature release level on a MetaFrame XP server**
  1. In the Management Console for MetaFrame XP, right-click the server and choose **Set Feature Release Level**.
  2. In the dialog box that appears, select the feature release level.
• If you select **Feature Release X**, the server attempts to acquire a Feature Release X product license from the license pool and the features of the feature release are available on the server. Do not set the feature release level if a feature release license is not available, because the server cannot accept connections from ICA Clients without the license.

• If you select **None**, the server does not acquire a Feature Release X license and the features of Feature Release X are not available on the server.

3. Click **OK** to set the feature release level.

**Migrating to MetaFrame XP**

MetaFrame XP can run in mixed mode, with MetaFrame 1.8 servers and MetaFrame XP servers coexisting in a single farm. Citrix recommends you use this mixed mode only during pilot deployments or migrations, not as a permanent solution. See “Interoperability with MetaFrame 1.8” on page 100 for more information about the limitations of mixed mode.

**Supported Migration Paths**

Starting with Feature Release 2, MetaFrame XP is no longer supported on Windows NT 4.0, Terminal Server Edition. Starting with Feature Release 3, MetaFrame XP is supported on Windows Server 2003, in addition to Windows 2000 Server.

MetaFrame XP supports the following paths for upgrading to newer versions of MetaFrame XP.

<table>
<thead>
<tr>
<th>Starting MetaFrame version</th>
<th>Upgrade path</th>
</tr>
</thead>
<tbody>
<tr>
<td>MetaFrame 1.8 for Windows NT 4.0, Terminal Server Edition, (at Windows NT SP 6)</td>
<td>MetaFrame 1.8 for Windows 2000 to MetaFrame 1.8 for Windows 2000 (at Windows 2000 SP 3) to MetaFrame XP with Feature Release 3 (includes Feature Releases 1 and 2 and Service Packs 1 and 2)</td>
</tr>
<tr>
<td>MetaFrame XP 1.0 for Windows NT 4.0, Terminal Server Edition, (at Windows NT SP 6)</td>
<td>MetaFrame XP 1.0 for Windows 2000 (at Windows 2000 SP 3) to MetaFrame XP with Feature Release 3 (includes Feature Releases 1 and 2 and Service Packs 1 and 2)</td>
</tr>
<tr>
<td>MetaFrame XP with Feature Release 1 on Windows NT 4.0, Terminal Server Edition (at Windows NT SP 6)</td>
<td>MetaFrame XP for Windows 2000 (at Windows 2000 SP 3) to MetaFrame XP with Feature Release 3 (includes Feature Releases 1 and 2 and Service Packs 1 and 2)</td>
</tr>
<tr>
<td>MetaFrame 1.8 at Service Pack 3 for Windows 2000 (at Windows 2000 SP 3)</td>
<td>MetaFrame XP with Feature Release 3 (includes Feature Releases 1 and 2 and Service Packs 1 and 2)</td>
</tr>
</tbody>
</table>
Overview of the Migration Process

If you want to migrate a MetaFrame 1.8 for Windows server to a MetaFrame XP server, complete the following tasks:

- **To migrate a MetaFrame 1.8 server farm to MetaFrame XP**
  1. Configure the database server if you are using Microsoft SQL Server, Oracle, or IBM DB2 for the MetaFrame XP server farm’s data store.
  2. Install MetaFrame XP on a server that is not the current master ICA Browser.
     - During MetaFrame XP installation, choose the option to create a new server farm.
     - Name the new MetaFrame XP server farm exactly the same as the existing MetaFrame 1.8 server farm.
  3. Using the Management Console for MetaFrame XP, install and activate the migration licenses you received in your MetaFrame XP migration kit.

This server becomes the new master ICA Browser, so it must be a server capable of handling the increased load. You can use the `query server` command-line utility to discover the MetaFrame XP server acting as the master browser. An **M** next to the network address of a server indicates that it is the master browser.

When the server restarts after MetaFrame XP installation, the browser election process causes published applications and server browsing to be temporarily unavailable. Therefore, it is best to do this initial migration outside of normal working hours.

---

**Starting MetaFrame version** | **Upgrade path**
--- | ---
MetaFrame XP 1.0 for Windows 2000 (at Windows 2000 SP 3) | MetaFrame XP with Feature Release 3 (includes Feature Releases 1 and 2 and Service Packs 1 and 2)
MetaFrame XP with Feature Release 1 for Windows 2000 (at Windows 2000 SP 3) | MetaFrame XP with Feature Release 3 (includes Feature Releases 1 and 2 and Service Packs 1 and 2)
MetaFrame XP with Feature Release 2 for Windows 2000 (at Windows 2000 SP 3) | MetaFrame XP with Feature Release 3
MetaFrame XP with Feature Release 2 for Windows 2000 (at Windows 2000 SP 3) | MetaFrame XP with Feature Release 3 for Windows Server 2003 (upgrade the operating system and then install MetaFrame XP with Feature Release 3)
4. Verify that you can connect to the MetaFrame XP server and check the migration log file to confirm that all applications were migrated successfully. MetaFrame XP Setup displays the name of the log file. The file is located in %SystemRoot%\System32.

5. Migrate additional MetaFrame 1.8 servers. During installation, choose to join an existing farm.

6. After all MetaFrame 1.8 servers are migrated to MetaFrame XP, change the server farm to operate in native mode by selecting the farm node and choosing Properties in the Management Console for MetaFrame XP. Clear the check box under MetaFrame Interoperability on the Interoperability tab. When you make this change, license sharing with license gateways stops. For more information, see “Pooling License Counts in Mixed Mode” on page 102.

**Cloning a MetaFrame XP Server**

If your organization uses system imaging utilities to clone standard server configurations, with a few adjustments you can also clone MetaFrame XP servers.

*Important* If you clone a MetaFrame XP server on which you have installed MetaFrame XP with a feature release, you must set the server’s feature release level to activate new features. For more information about setting a feature release level on a MetaFrame server, see “Setting a Server’s Feature Release Level” on page 130.


**Uninstalling MetaFrame XP**

If you want to remove a MetaFrame XP server from a server farm, Citrix recommends that you uninstall MetaFrame XP. This removes the host information from the server farm’s data store and removes the server from the list of servers displayed in the Management Console for MetaFrame XP.

You can uninstall MetaFrame XP using Add/Remove Programs in Control Panel or using the Windows Msiexec command. For more information about this command, go to the Microsoft Web site and search on “msieexec.”

Before uninstalling MetaFrame XP, log off any ICA sessions and exit all programs running on the server.
To uninstall MetaFrame XP

1. Exit any applications running on the server.
2. Choose Start > Settings > Control Panel > Add/Remove Programs.
3. Click Change or Remove Programs, select Citrix MetaFrame XP, and click Remove.

If you need to force the removal of MetaFrame XP from the system, you can use the command line to add the property

**CTX_MF_FORCE_SUBSYSTEM_UNINSTALL**

and set its value to “Yes.”

The following sample command line enables logging of the uninstallation operation and forces the removal of MetaFrame XP:

```
msiexec /x MFXP001.msi /L*v c:\output.log
CTX_MF_FORCE_SUBSYSTEM_UNINSTALL="Yes"
```

---

**Important** If you rename a MetaFrame XP server on your network, the new server name is added to the list of MetaFrame XP servers in the server farm. However, you must remove the old server name because it is still listed as a member of the server farm. Before you remove the server name, be sure to update all references to the new server name, including data collector ranking, published application references, and license assignments.

If you are planning to uninstall MetaFrame XP from the Resource Manager metric farm server or database connection server for a summary database, be sure to reassign the server before removing it from the farm. If you are using a summary database, Citrix recommends that you update it before removing any servers from the server farm. Be sure to also create any necessary billing reports from the server before you remove it.

---

**Installing the Management Console for MetaFrame XP on Other Computers**

The Management Console for MetaFrame XP is a centralized management utility you use to administer a MetaFrame XP server farm. The console is automatically installed on MetaFrame XP servers when you install MetaFrame XP.

You can use the MetaFrame XP CD to install the Management Console on workstations that do not have MetaFrame XP installed. For compatibility information, see “Management Console for MetaFrame XP Requirements” on page 47.
To install the Management Console for MetaFrame XP on other computers

1. Exit all applications.
2. Insert the MetaFrame XP CD-ROM in the CD-ROM drive.
   - If your CD-ROM drive supports Autorun, the MetaFrame XP splash screen appears.
   - If the splash screen does not appear or you are installing from a network share point, choose Start > Run and type d:\autorun.exe, where d is the letter of your CD-ROM drive or network share point.
3. Select Other tools and components > Administration tools > Management Console.
4. Follow the instructions in the Setup wizard.

Updating the Management Console for MetaFrame XP

When you upgrade to a newly released feature release or service pack, Setup updates the Management Console on a MetaFrame XP server. To update the console on a system that is not a MetaFrame XP server, click Other tools and components on the Autorun screen and then click Administrative Tools > Management Console.
Chapter 5

Licensing MetaFrame XP

This chapter describes licensing for MetaFrame XP and its feature releases and service packs. It includes an overview of licensing requirements and describes various types of licenses.

To find step-by-step instructions for procedures mentioned in this chapter—including how to enter, activate, and assign licenses—use online help in the Management Console for MetaFrame XP.

For information about **CLICENSE**, a command-line utility that you use to view and change licensing data on MetaFrame XP servers, see “CLICENSE” on page 333.

For information about **MLICENSE**, a command-line utility that you use to add, activate, and back up multiple licenses in a MetaFrame XP server farm, see “MLICENSE” on page 351.

**Overview of MetaFrame XP Licensing**

Using Citrix MetaFrame software requires that you follow the terms of Citrix MetaFrame license agreements. Usually, you purchase a license that permits the software to be used on a specified number of servers and permits a specified number of ICA connections to the MetaFrame XP servers.

In addition to the legal agreement, the term *license* refers to codes and software that enable Citrix MetaFrame products to operate. Software mechanisms verify the presence of valid licenses for Citrix MetaFrame products in MetaFrame XP server farms.

For details about licensing requirements and licensing terms for your Citrix MetaFrame product, be sure to read to the End-User License Agreement that is provided with the software package in printed or electronic form.
Important  If your organization participates in a Citrix MetaFrame enterprise licensing program or ASP licensing program, Citrix provides additional software and documentation for license metering and reporting. If your organization participates in an enterprise program, do not follow the licensing instructions in this chapter; instead, refer to your enterprise license documentation or ask your enterprise sales representative for the detailed enterprise licensing information.

Summary of the Licensing Process

The steps below summarize the general process you use for MetaFrame XP licensing. Whether your server farm is small or large, the general steps you use to enter and activate licenses are the same.

For definitions of the licensing terms used in the following procedure, see “Understanding MetaFrame XP Licensing Codes” on page 142.

To enter licenses for Citrix MetaFrame XP products

1. Get the product code and serial number from your MetaFrame XP product packaging.
   - Make product codes and serial numbers available to administrators who manage licensing for the server farm.
   - Store the original product codes and serial numbers in a safe place.

2. When you install MetaFrame XP on a server and select a product type, the corresponding product code is automatically referenced. Verify that the product code matches the product code in your product packaging. If you did not receive a product code in your product packaging, accept the suggested product code.

3. Use the Management Console for MetaFrame XP to enter the serial numbers for all of your MetaFrame XP licenses. For each serial number you enter, a license description and license number appear on the License Numbers tab in the console.

4. When you enter a license in the Management Console, you must then activate the license. In a Web browser, go to the Citrix Activation System (CAS) Web page at http://www.citrix.com/activate. Paste the license number into the text box and then copy the activation code you receive for the license.
5. Enter the activation code in the **Activate License** dialog box and click **OK** to activate the license. Check the **License Numbers** tab to be sure you activate all licenses.

You can use **Mlicense**, a command-line utility, to add, activate, and back up multiple licenses in a MetaFrame XP server farm. See “MLICENSE” on page 351 for more information.

6. After you enter and activate licenses, MetaFrame XP pools all license counts in the server farm. Through the farm’s data store, license counts are allocated from the pool to MetaFrame XP servers in the server farm that require product and connection license counts. You can use the Management Console to monitor license usage by the entire farm and by individual servers.

7. If you want to assign activated licenses to specific servers, use the New Assignment wizard to assign product and connection license counts to any MetaFrame XP server in the farm. License counts that you assign are taken out of the pool of unassigned licenses. You cannot assign licenses that are not activated. For more information about product and connection licenses, see “Product Licenses” on page 140 and “Connection Licenses” on page 141.

---

**Important** The Management Console does not verify that license counts you assign to a server are the correct type specified by the server’s product code. If you assign a license count from a MetaFrame XPs license, for example, and the server’s product code specifies MetaFrame XPe licensing, the server cannot use the assigned license count. The unused count is not returned to the license pool, and therefore, is not available for use in the server farm.

---

**Grace Periods for License Activation**

After you enter a license serial number, you can use the software during a grace period before you must activate the license.

For MetaFrame XP licenses, refer to the Grace Days column on the **License Numbers** tab in the Management Console. The numbers in this column tell you the number of days that remain in the grace period for each license. Before a grace period ends, you must activate the license.

Citrix recommends that you use the grace period to thoroughly test your hardware and software configuration. When you are sure your system is set up properly, you can permanently activate your licenses.

Demonstration licenses and evaluation licenses must be activated using the same procedure described above. However, these licenses are valid for a limited period even after activation.
Types of MetaFrame XP Licenses

Two types of licenses appear in MetaFrame XP licensing: product licenses and connection licenses. When you manage licenses for MetaFrame XP, you work with both types of licenses. In some procedures, you need to specify one type of license.

A MetaFrame XP license can provide either a product or a connection license alone, or both types of licenses together. A serial number that provides product and connection licenses together can include no more than one license count for the product license. If you add more servers to a server farm, you can obtain a product license with the license count you need for the additional servers. For more information about license counts, see “Managing License Counts” on page 152.

Product Licenses

A *product license* is a license to use one or more Citrix MetaFrame XP products on your servers. A server farm must have a product license with one license count to run Citrix MetaFrame XP software on each server in the server farm.

The table below describes the product licenses that are available to enable Citrix MetaFrame XP Server for Windows and related MetaFrame XP products.

<table>
<thead>
<tr>
<th>Product license</th>
<th>Products enabled</th>
</tr>
</thead>
<tbody>
<tr>
<td>MetaFrame XPs</td>
<td>MetaFrame XP, the Web Interface for MetaFrame XP</td>
</tr>
<tr>
<td>MetaFrame XPa</td>
<td>MetaFrame XP with Load Manager, the Web Interface for MetaFrame XP</td>
</tr>
<tr>
<td>MetaFrame XPe</td>
<td>MetaFrame XP, Load Manager, the Web Interface for MetaFrame XP, Resource Manager, Installation Manager, Network Manager</td>
</tr>
</tbody>
</table>

As mentioned above, a license serial number can include both product and connection licenses. For more information, see “Connection Licenses” on page 141.

When you add a MetaFrame XP license to your server farm, the product license provided by the license number appears on the *Product* tab in the Management Console. Only one product license appears on the tab, even if the product license—such as a MetaFrame XPa product license—enables more than one Citrix MetaFrame XP product.

MetaFrame XP allocates product licenses from a pool of available licenses for a MetaFrame XP server farm. To monitor the product licenses in a farm, select *Licenses* in the tree pane and use the *Product* tab in the Management Console.
A server does not consume a product license when it is not in operation—when the server is down or the IMA service is not running. When a server releases a product license, the license returns to the license pool and is available for use by another server.

With a MetaFrame XPa or MetaFrame XPe product license, which enables multiple products on your servers, you cannot divide the product license to enable one product on one server and other products on other servers.

**Connection Licenses**

A *connection license* is a license for ICA Client connections to MetaFrame XP servers. Because of the client device licensing feature, one connection license count in the license pool supports multiple concurrent ICA sessions from one client device to the MetaFrame XP server farm.

Each MetaFrame XP product license provides one grace license for the administrator to connect to the server console. The grace license prevents the server from reporting a licensing error if you install no connection licenses and log on to the server before putting it into service for ICA Clients.

License serial numbers that you receive with MetaFrame XP can provide connection licenses alone or in combination with a MetaFrame XP product license. If you add more users, you can get additional connection licenses with the license count you require.

**Migrating Licenses from Earlier Versions of MetaFrame**

MetaFrame XP does not directly support licenses for MetaFrame 1.8, *WINFRAME* 1.8, and earlier versions of MetaFrame or *WINFRAME*. However, you can use licenses from earlier versions of MetaFrame if you purchase the appropriate product migration licenses.

You can enter MetaFrame and *WINFRAME* product licenses in your server farm’s data store using the Management Console for MetaFrame XP.

If you install MetaFrame XP on servers running earlier versions of MetaFrame, Setup migrates existing licenses into the new MetaFrame XP server farm.

---

**Important** If you cannot preserve your original licenses on a MetaFrame XP server because you cannot upgrade the operating system or you perform a clean install of the operating system or MetaFrame XP, you must enter the original license serial numbers in the Management Console and then reactivate the licenses before they can be used with a migration license.

---

MetaFrame XP supports migration of licenses from the following products:
You can migrate earlier product licenses to MetaFrame XPs, MetaFrame XPa, and MetaFrame XPe product licenses.

**Important** If you enter migration licenses in your server farm, you might need to change the product code. A server will not use a migration license if the server’s product code is different from the product code of the migration license. For more information, see “Product Codes” on page 143.

When a server starts, it requests a product license from the server farm’s license pool. If the server’s product code allows it to take a migration license, it can use a migration license from the license pool if it can also get a corresponding original license for the migrated product.

### Upgrading Licenses

You can upgrade your MetaFrame XP servers to enable more features by installing additional software and entering MetaFrame upgrade licenses into the server farm’s license pool. For example, you can upgrade MetaFrame XPs to MetaFrame XPa or MetaFrame XPe by installing the MetaFrame XP software included with the upgrade licenses and entering the licenses in the server farm.

If you upgrade a server, you must change the server’s product code to match the product code of the upgrade license. For example, if you upgrade a server from MetaFrame XPs to MetaFrame XPa, you must change the server’s product code to the one included with the MetaFrame XPs-to-MetaFrame XPa upgrade license.

### Understanding MetaFrame XP Licensing Codes

Licensing for Citrix MetaFrame XP Server and related MetaFrame XP products involves several licensing codes, which are strings of characters that you use during the licensing process. You get some licensing codes from your MetaFrame XP software package and software generates other strings that you use in connection with MetaFrame XP licensing.
Product Codes

Each Citrix MetaFrame XP software package includes a *product code*. The product code is an alphanumeric string of nine characters that:

- Identifies the MetaFrame XP software product
- Distinguishes among retail, evaluation, and not-for-resale product versions
- Specifies the product license a server requests from the license pool to enable the installed MetaFrame XP software

The product code for MetaFrame XP appears on a label on the product package. One or more license serial numbers are also on the label.

### Allocating License Counts According to Product Codes

With MetaFrame XP, license counts are allocated to individual servers from a common license pool for the server farm. The automatic allocation of licenses means you do not have to manually assign licenses to servers.

A variety of MetaFrame XP licenses, including evaluation, migration, upgrade, and full retail licenses can exist in the license pool. The product code applied to a server specifies the kind of product license count the server takes from the license pool.

For example, you might have evaluation and full retail licenses in your server farm’s license pool. You install evaluation applications on some servers and install production applications on other servers. In this scenario, you do not want evaluation servers to take retail licenses away from production servers. Therefore, you enter product codes to specify which servers require retail license counts and which servers can use evaluation license counts.

In addition to evaluation and retail licenses, product codes distinguish among MetaFrame XPs, MetaFrame XPa, and MetaFrame XPe licenses. Without the correct product code on a server (and corresponding license counts available in the pool), the MetaFrame XP software will not function on a server.

For example, if you specify a MetaFrame XPs product code and no MetaFrame XPs license counts are available, the server will not take a MetaFrame XPa or MetaFrame XPe license count if these licenses are in the license pool.
If you install MetaFrame XP and Installation Manager on a server and enter the MetaFrame XPs license code, for example, the server will request a MetaFrame XPs license count from the license pool. Even if the license count is available, Installation Manager will not be enabled on the server because a MetaFrame XPs license enables only MetaFrame XP to run on the server.

**Changing a Server’s Product Code**

You can change a product code to change a server’s product license specification. Adding a license to the server farm’s license pool does not change the product code on any servers.

For example, you might want to change the product code to convert an evaluation server to use a full license. Another example is to change the product code when you upgrade a server that uses a MetaFrame XPs license to use a MetaFrame XPa license and enable Load Manager features.

- **To change a server’s product code**
  1. Select the server in the Management Console.
  3. Enter the product code and click OK.

**Tip** To select multiple servers so you can change their product codes at once, select the Servers node in the Management Console and then select the servers on the Contents tab.

When you change the product code, a status bar indicates the progress of the change. The process can last several minutes if you change the product code on many servers at once. The status bar indicates when the product code change is complete on all the selected servers.

**Serial Numbers**

A **serial number** is the code that you enter in the first step of the licensing process, using the Management Console for MetaFrame XP.

The serial number represents the exact licenses you purchased. MetaFrame XP uses the serial number to identify and validate your licenses.

The serial number is on a label in the MetaFrame XP software package. A MetaFrame XP serial number is a string of 25 letters, numbers, and symbols. The string has five groups of five characters each, with a hyphen between each group.
Tip The licensing label in your product package might include more than one serial number, depending on the particular MetaFrame XP licenses that you purchase. A serial number for a connection license is labeled “ICA Connect.” A serial number for a product license is labeled “Server.”

Representation of Licenses by Serial Numbers

Serial numbers for MetaFrame XP can represent the following types of MetaFrame XP licenses:

Product license. MetaFrame XPs, MetaFrame XPa, and MetaFrame XPe product licenses enable the use of Citrix MetaFrame XP Server for Windows and MetaFrame XP management products on servers. Each license enables particular MetaFrame XP products and features on servers (see the table on page 140 for more information).

The number of servers that a product license allows depends on the license count.

Connection license. This license enables concurrent connections by ICA Client users to MetaFrame XP servers. The number of concurrent connections allowed by the license depends on the license count.

Types of Licenses Provided by a Serial Number

A MetaFrame XP license serial number can represent a single MetaFrame XP license or a combination of licenses. However, some license combinations cannot be represented by a single serial number. A single serial number can represent only the following:

- A product license (MetaFrame XPs, MetaFrame XPa, or MetaFrame XPe) that includes multiple license counts for multiple servers
- A connection license that includes multiple license counts for concurrent ICA connections
- A product license with one license count plus a connection license with multiple license counts

For example, one serial number can represent a MetaFrame XPs product license with a single license count and a MetaFrame connection license with a 15-connection license count. Another serial number can represent a MetaFrame XPe product license with a 500-server license count.
To enable MetaFrame XP and MetaFrame XP management products for the number of servers and connections that you use in a server farm, you need to obtain a product license with a license count equal to (or greater than) the number of servers you have, and a MetaFrame connection license with a license count equal to (or greater than) the number of concurrent ICA connections your users require.

### Entering Serial Numbers

To add licenses to your server farm, you enter license serial numbers during installation of MetaFrame XP or with the Management Console.

After you enter serial numbers, the Management Console produces a license number from each serial number. You use the license number to receive an activation code from Citrix for the licenses.

All types of MetaFrame XP licenses require activation within a set period of time, which is called the *grace period* and typically lasts 90 days. Licenses that you do not activate during the grace period expire and are invalid. Evaluation licenses require activation but are valid for a limited period, typically 90 days after activation.

### License Numbers

A *license number* is a code that you use in the licensing process for MetaFrame XP and MetaFrame XP management products. License numbers are strings of letters, numbers, and symbols.

For licensing of MetaFrame XP and other IMA-based products, you use a license number that is derived from each serial number you enter in a server farm. The Management Console displays each license number, which consists of the original serial number plus additional characters; these additional characters are referred to as the *machine code*.

You use license numbers to get activation codes, as described below, for each MetaFrame XP license.

### License Activation Codes

All types of MetaFrame XP licenses require activation. To activate a license, you enter the *activation code* for the license in the Management Console for MetaFrame XP. The activation code is a string of characters that you get from the Citrix Activation System (CAS) Web page. You can use the CAS system with any Web browser and Internet connection. For more information, see “Activating Licenses” on page 148.

Each activation code is a unique string that activates only one specific license number.
Managing and Monitoring Licenses

In a MetaFrame XP server farm, the data store for the farm contains all data associated with licensing for the farm, including the types of licenses you enter, their license numbers, license counts, and license assignments to specific servers.

You use the Management Console to monitor and manage licensing for MetaFrame XP servers and connections by ICA Client users. With the console, you can do the following:

- Add licenses to a server farm
- Activate licenses
- Monitor usage of product and connection license counts
- Assign license counts to specific servers
- Remove licenses from a server farm
- Copy license numbers for use in the CAS system

For information about the basics of using the Management Console, see “To use the Management Console” on page 177.

For information about Mlicense, a command-line utility that you use to add, activate, and back up multiple licenses in a MetaFrame XP server farm, see “MLICENSE” on page 351.

The Management Console communicates with the data store in a server farm to display information about licenses in the farm. When you make changes by adding or removing licenses, or changing license assignments, the console updates the licensing data in the farm’s data store through the Citrix IMA protocol.

---

**Important** When you view information about license usage, use the Refresh command to be sure the information is current. When ICA Clients connect or disconnect from the farm, the licensing data is not updated automatically. Use the Refresh command to ensure that connection license data is current.

Similarly, MetaFrame XP does not refresh the data in the console when servers are brought online or go offline. Use the Refresh command to be sure that license usage data is current when you view product license information in the Management Console.

---

To set automatic refresh of licensing data

You can specify an interval for automatic refresh of licensing data displayed in the Management Console. If you do not select the automatic refresh setting, licensing data is not refreshed unless you choose the Refresh command or a license change event, such as adding or removing a license from the server farm, occurs.
1. Select the License node in the console tree.
2. Choose Preferences from the View menu.
3. On the License Data tab of the Preferences dialog box, select Automatically refresh licensing data, enter the refresh interval in seconds, and click OK.

Adding Licenses to Server Farms

To add a license to a MetaFrame XP server farm, you enter a license serial number that you receive with a MetaFrame XP product.

Use the Management Console for MetaFrame XP to enter each serial number for licenses that you want to use in the farm. Choose New > License from the Actions menu or click the Add License button on the toolbar to begin entering a license.

Type MetaFrame XP serial numbers exactly as they are printed, including hyphens (dashes) between the groups of characters. The characters in a serial number can include numerals, letters, and symbols such as + (plus sign), ? (question mark), and * (star).

After you enter a serial number, the license appears on the License Numbers tab. The license number that is shown on the tab is the serial number that you entered, followed by 12 additional characters that the licensing subsystem generates.

When you first enter a license, the license is not activated. The Status column on the License Numbers tab displays Unactivated and the Grace Days column shows the number of days remaining before the license will expire if you do not activate it.

When you enter an unactivated license, the console asks if you want to activate the license.

Activating Licenses

You must activate each MetaFrame XP license to complete the licensing process for MetaFrame XP software and ensure continued operation. While a license is not activated, reminder messages appear on the MetaFrame XP server console.

If you do not activate a license, the license expires after a set grace period. When a license expires, the license is no longer valid. An invalid license prevents users from connecting to the MetaFrame XP server. In addition, you cannot assign unactivated licenses to servers.

To activate a license, you obtain an activation code and then enter the code in the Management Console.

Tip  You can right-click a license number on the License Numbers tab and choose Activate to start the activation process.
To activate licenses using the Web

1. Select a license number on the License Numbers tab in the Management Console for MetaFrame XP and choose Actions > Activate.
2. In the Activate License dialog box, click Copy to Clipboard to copy the license number to the Clipboard for the next step.
3. Go to the Citrix Activation System Web page at http://www.citrix.com/activate. Enter the license number. The CAS page returns the activation code for the license number.
4. Copy the activation code, enter the activation code in the Activate License dialog box, and click OK to activate the license.

After you activate a license, the Status column displays Activated on the License Numbers tab. The license number remains the same because activation codes do not appear as part of the license number.

Note Licensing changes might not appear immediately in the Management Console. To refresh the display after adding or activating a license, press F5 or choose View > Refresh.

To activate licenses by phone

If you cannot use the Web for license activation, you can get an activation code by phone.

1. Select a license number on the License Numbers tab in the Management Console and choose Activate from the Actions menu, the right-click menu, or the toolbar.
2. Write down the license number that appears in the Activate License dialog box. You can leave the dialog box open for the following step.
3. Call (800) 424-8749 to speak with a customer service representative and get an activation code.
4. After you obtain an activation code, enter the activation code in the Activate License dialog box and click OK to activate the license.

License Views

To monitor and make changes to licensing in your server farm, you primarily use the Licenses node in the Management Console for MetaFrame XP.

When you select the Licenses node in the console’s left pane, you can use the Product, Connection, and License Numbers tabs that appear in the right pane to monitor license usage and configuration.
Displaying License Numbers

The License Numbers tab lists each license that you enter in the server farm. Each license that appears on the tab is based on a single license number, which you can view in the License Number column. The tab also shows which licenses are activated and unactivated, and the grace period for unactivated licenses.

This tab can display multiple licenses with the same description; the License Numbers tab does not consolidate licenses based on product or license type.

For example, if you enter three serial numbers that represent licenses for MetaFrame XP 1.0 for Windows, each license appears in the list on the License Numbers tab. Two licenses might contribute both product and connection licenses, while the third might add license counts for additional servers in the farm.

To see what licenses a license number contributes to the server farm, double-click the license in the list.

Use the Copy to Clipboard command to copy the license number of any license you select in the list. You can paste the data from the Clipboard into other applications for reporting and archiving.

Monitoring Connection Licenses

The Connection tab lists MetaFrame XP connection licenses. The tab shows the license count, which is the number of concurrent ICA connections allowed by the license, and usage data for each connection license you enter.

More than one serial number can contribute to one type of connection license. Each type of connection license—such as MetaFrame Connection—appears only once on the tab.

For example, “MetaFrame Connection” appears once on the Connection tab, even if you enter multiple serial numbers that include connection licenses. Additional licenses increase the license count, which appears in the Count column.

Use the Properties command (or double-click a license in the list) to display additional details about a connection license. You can monitor the use of the connection license by servers in the farm. You can also see the license number that includes the connection license, check the status of the license, and see how many grace days remain before you must activate a license that is not activated.
Chapter 5 Licensing MetaFrame XP

Monitoring Product Licenses

The **Product** tab lists MetaFrame XP product licenses. The tab shows the license description, the license count (the number of servers allowed by the license), and usage data for each product license you enter.

If you enter multiple license serial numbers, each distinct MetaFrame XP product appears once on the **Product** tab. Additional licenses can increase the license count for a product without adding additional product licenses to the list.

<table>
<thead>
<tr>
<th>Connection</th>
<th>Product</th>
<th>License Numbers</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>MetaFrame XP 1.0 English for Windows</td>
<td></td>
</tr>
</tbody>
</table>

For example, “MetaFrame XP 1.0 English for Windows” is one distinct product license. If you enter more than one serial number for this license, the product description appears once. The Count column shows the total license count for the product license.

Use the **Properties** command or double-click a license description in the list to display additional details about a product license. In the **Properties** dialog box, you can monitor the use of the product license by servers in the farm. You can also see the license number that includes the product license, check the status of the license, and see how many grace days remain before you must activate a license that is not activated.

Monitoring Server Information

You can select individual servers in the console tree to view licensing information for each server.

When you select one server in the tree, the **Licenses** tab appears in the console’s right pane. This tab shows any license counts that are in use by the server, as well as any license counts assigned to the server.

License counts that you assign to a server are removed from the license pool; an assigned license is available only to the server on which it is assigned. An assigned license is not available to other servers, even if the license is not in use because the server is down. For more information, see “Assigning License Counts” on page 153.
Important  In a mixed server farm environment, the Management Console monitors and manages licensing data for MetaFrame XP servers only. To change license data on MetaFrame 1.8 servers, use the licensing commands and utilities that ship with that product; these utilities are also included on the MetaFrame XP CD-ROM for your convenience. The MetaFrame 1.8 licensing commands do not report or configure licensing data for MetaFrame XP or other IMA-based servers.

Note  Licenses that are migrated into the server farm from earlier Citrix Products, such as Load Balancing Services and SecureICA Services, will appear in the Management Console, even though the licenses are not used in the MetaFrame XP server farm.

Managing License Counts

Product licenses and connection licenses each include a license count. The license count is the number of products or connections that the license authorizes.

For example, a connection license with a license count of 50 allows 50 concurrent ICA connections to the server farm.

License counts appear in the Count column on the Product and Connection tabs in the Management Console for MetaFrame XP. These tabs display similar licenses as single items in the list. These single items are called license sets. A license set includes the total license count from all licenses in the set.

For example, you might have two MetaFrame XPs licenses, one with a license count of 15 and one with a license count of 20. When you enter these licenses in your server farm, just one license set with a license count of 35 appears on the Product tab.

The Management Console uses license count data wherever it displays license usage information. The numbers that are labeled “pooled” and “in use” refer to license counts that are pooled and in use.

Note  For some types of MetaFrame XP product licenses, the license count is unlimited, which means that the license authorizes the installation and use of the product on any number of servers.
Pooling License Counts

To simplify management of licenses, MetaFrame XP always combines the license counts for each product license into a common pool for the server farm. It does the same with the license counts for connection licenses.

By default, all MetaFrame XP servers in the farm can take license counts from the license pools as needed for new connections and new servers.

For example, as more users connect to a MetaFrame XP server, the server takes connection license counts from the license pool. If you restart a farm server that was offline, the server takes a product license count from the license pool when it begins operating in the farm.

**Important** The product license count that a server takes from the license pool depends on the product code assigned to a server. A server does not take product license counts from licenses other than the license specified by its product code. For example, if a server’s product code specifies MetaFrame XPe, the server does not take a MetaFrame XPs or MetaFrame XPa license count from the license pool.

Assigning License Counts

The only license counts that are not available to all servers are license counts that you explicitly assign to specific servers.

If you assign license counts to a server, you remove the specified count from the pool and dedicate the count to one server only. You can do this with most licenses, but you cannot assign some types of licenses, including unactivated, demonstration, and evaluation licenses.

You can assign licenses to servers based on the type of applications published in the farm and the number of servers that host mission-critical applications.

For example, if you assign connection license counts to certain servers and you set up certain ICA Clients to connect to those servers, you can be sure of the number of users who can connect to that group of servers. While the license pool for the server farm might run out of connection license counts at some times, the servers to which you assigned license counts will always have the number that you specified.

You use the New Assignment wizard in the Management Console to assign product and connection license counts. Select a license set on the **Connection** or **Product** tab, and choose **License > New Assignment** from the **Actions** menu to begin the process.

The wizard guides you to select a specific server in the farm and then to specify the license count to assign to that server. Repeat the process if you want to assign more license counts to other servers in the farm.
Changing License Assignments

To change a server’s license count assignment, you select the server in the Management Console and select the license set on the Licenses tab. Use the Change Assignment command to adjust the license count.

If you reduce the license count that is assigned to a server, you return the count to the license pool for use by all servers in the farm.

You can remove the assigned license counts from a server by selecting the license set and choosing the Drop Assignment command.

Removing Licenses

Normally, you do not remove licenses from a server farm. However, you might want to remove a license if it expires, or if you want to replace an evaluation license with a full product license.

To remove a license, select it on the License Numbers tab in the Management Console and choose License > Remove from the Actions menu.

Client Device Licensing

Client device licensing is a feature that allows users to start multiple sessions on the same or different servers while using only a single MetaFrame XP license count. The user must make all connections from a single client device.

When a user starts a second session on the same MetaFrame XP server, the new session does not consume a second connection license count. If the user starts a second session on a different server, the new session does not consume a second connection license count if the first session used a pooled license count.

Licensing Requirements for MetaFrame XP Feature Releases

MetaFrame XP feature releases include new features that require licensing. To enable MetaFrame feature releases, you must add feature release product licenses and feature release connection licenses to the server farm.

Feature release product licenses. Most product licenses have an unlimited license count, which means the license can be used by all the MetaFrame XP servers in a server farm. You must install a feature release product license in the server farm to make the features of the feature release available. Each MetaFrame XP server that has its feature release level set to the latest feature release requests a feature release product license count from the server farm’s license pool.
Feature release connection licenses. Each ICA session between an ICA Client and a MetaFrame XP, Feature Release X server requires one feature release connection license count. Subsequent connections to the same server do not use an additional license count.

In addition, subsequent connections to a different server in the same farm do not use an additional license count if the first session used a pooled feature release connection license. If the feature release level of a MetaFrame XP server is set to Feature Release X, the server requests a Feature Release X connection license count from the license pool.

Important Configuring a MetaFrame XP server to use Feature Release X without installing the required licenses makes the server unable to accept connections from users. If a server’s feature release level is set to Feature Release X, but Feature Release X product and connection licenses are not installed, users cannot connect to the server and run ICA sessions.

You can disable the feature release on a server by setting the feature release level to “Not Installed.” For more information, see “Setting a Server’s Feature Release Level” on page 130.

MetaFrame XP licensing terms can differ for enterprise customers, retail customers, evaluation software, and not-for-resale products packages. For information about the specific terms and conditions of your license, refer to the End-User License Agreement that is included with the software or license package.

To add feature release licenses to a server farm

1. Log on to the Management Console for MetaFrame XP by choosing Start > Programs > Citrix > Citrix Management Console.

Important To add licenses, you must be a MetaFrame XP administrator with rights to perform licensing tasks.

2. Choose Actions > New > License or click Add License on the toolbar. The Add License dialog box appears.

3. In the Add License dialog box, type a MetaFrame XP license serial number exactly as it appears. Include all hyphens (dashes) between the groups of characters. The serial number can include numerals, letters, and symbols such as plus signs, question marks, and stars.

Click OK after you type the license serial number.
4. A message confirms successful installation and prompts you to activate the license. Click Yes to activate the license at this time or No to activate the license later.

5. Repeat Steps 2 through 4 for each license you want to add to the server farm. After you add licenses to the server farm, be sure to activate the licenses as described next.

**Note** To add and activate multiple licenses in a server farm, use the mlicense utility. See “Using Mlicense to Add, Activate, and Back Up Licenses” on page 354 for more information.

### Activating Feature Release Licenses

After you install MetaFrame XP licenses, you must activate each license to complete the licensing process. If a license is installed but is not activated, the MetaFrame XP server displays messages to remind you to activate the license.

If you do not activate a license, the license expires after a set period. If a license expires, the license is no longer valid. Lack of a valid license can prevent users from connecting to MetaFrame XP servers. You cannot assign non-activated licenses to servers.

### Viewing Feature Release License Information

When you install a feature release, the Management Console for MetaFrame XP displays information about the servers that are configured to use the feature release. The console also displays information about feature release licenses and license counts in use in the server farm.

When you select the Licenses node in the console, the tabs in the right pane display the following information related to licensing:

#### Viewing License Numbers

The **License Numbers** tab displays each license number that is added to the server farm. A license number consists of a license serial number followed by an eight-character code. A license number can be associated with a product or connection license for the base product (MetaFrame XP) or a feature release.
Viewing Feature Release Product Licenses

The **Product** tab displays information about MetaFrame XP product licenses, including feature release product licenses, that are in the server farm’s license pool. You can use this tab to check the number of servers that are using a feature release product license. Add the values in the Pooled in Use and Assigned in Use columns to calculate the total number of servers that are using a feature release product license.

If the number of servers that use a feature release license is less than you expect, check the feature release level that is specified on each server. A server does not attempt to acquire a feature release product license if its feature release level setting is “Not installed.” For more information, see “Setting a Server’s Feature Release Level” on page 130.

**Server configuration.** The lower pane of the **Summary** tab displays each feature release that servers in the server farm are configured to use.

The appearance of a feature release on the **Summary** tab is not based on whether or not feature release licenses are installed in the server farm. If you install a MetaFrame XP feature release or you set the feature release level manually on any server in the farm, the feature release name appears on the **Summary** tab, even if no feature release licenses are installed.

The lower pane of the **Summary** tab also displays the following information:

- The value in the Server Count column is the number of servers whose feature release level is set to the feature release listed in the first column. The data is not based on the licenses installed or in use in the server farm.
- The value in the Connection Count column is the total license count that is installed in the server farm for the listed feature release. If you install feature release connection licenses with license counts of 25 and 50, for example, this column displays 75.

**Note** The **Connection** tab displays base MetaFrame XP connection licenses; it does not display installed feature release licenses. However, if feature release connection licenses are installed, the total connection license count appears in the Connection Count column in the lower pane of the **Summary** tab, as described above.
Securing MetaFrame XP Deployments

Overview of Securing MetaFrame XP Deployments

Depending on your security needs, you can incorporate the following security components when designing secure MetaFrame XP deployments.

The guidelines outlined in this chapter are intended to provide general direction when planning secure MetaFrame XP environments. Be sure to consult with your organization’s security expert for a comprehensive security strategy that best fits your needs.

**Citrix SSL Relay.** Use Citrix SSL Relay to provide end-to-end Secure Sockets Layer/Transport Layer Security (SSL/TLS) encryption between specific MetaFrame XP servers and ICA Clients.

In general, you should use SSL Relay when:

- You have a small number of MetaFrame servers to support (five or fewer)
- You do not need to secure access at a DMZ
- You do not need to hide server IP addresses, or you are using Network Address Translation (NAT)
- You do need end-to-end encryption of data between ICA Clients and MetaFrame servers

**The Secure Gateway for MetaFrame.** Use the Secure Gateway to provide SSL/TLS encryption between a secure Internet gateway server and an SSL-enabled ICA Client, combined with encryption of the HTTP communication between the Web browser and the Web server. Using the Secure Gateway for MetaFrame makes firewall traversal easier and provides heightened security by providing a single point of entry and secure access to your MetaFrame XP server farms.
In general, you should use the Secure Gateway for MetaFrame when:

- You have a large number of servers to support
- You want to hide internal IP addresses
- You want to secure access from the DMZ
- You need two-factor authentication (in conjunction with the Web Interface)
- You need non-intrusive ICA Client installations; for example, users need access from Internet cafes

**ICA Encryption (Secure ICA).** Use ICA Encryption (Citrix SecureICA) to encrypt the information sent between a MetaFrame XP server and an ICA Client. ICA Encryption makes it virtually impossible for unauthorized users to open an encrypted transmission and, in the unlikely event that such an attack succeeds, ICA Encryption ensures that the attacker sees only meaningless screen commands and not sensitive information. ICA Encryption provides confidentiality to guard against the threat of eavesdropping.

**Note** ICA Encryption is not recommended for use across public networks.

In general, you should use ICA Encryption when:

- You want to secure internal communication within a LAN or a WAN, or you want to secure internal access to an Intranet
- You need to secure communications from devices that use Microsoft DOS or run on Win16 systems
- You have older devices running ICA Client software that cannot be upgraded
- There is little risk of “man-in-the-middle” attacks

**A Virtual Private Network Solution.** Use a Virtual Private Network (VPN) solution when you need to create secure tunnels between geographic locations.

In general, you should use a VPN solution when:

- You need two-factor authentication
- You need to create a secure pipeline for full (beyond ICA) network access
- You want to secure the network from within the DMZ
- Users normally access the network from the same workstations
- You want to use IP Security (IPSEC)
Both the Secure Gateway and SSL Relay support SSL/TLS encryption. Selection is largely a matter of deciding which topology best meets the needs of the organization’s security policies. Each approach has its own advantages.

An overview of the SSL Relay, the Secure Gateway, and ICA Encryption is included in this chapter.

**Overview - Deploying SSL Relay**

This deployment provides end-to-end encryption of the communication between the ICA Client and the MetaFrame XP server. You must install and configure SSL Relay and the appropriate server certificate on each MetaFrame XP server within the server farm.

The SSL Relay operates as an intermediary in the communications between the ICA Client and the XML service running on each MetaFrame XP server. Each client authenticates the SSL Relay by checking the Relay’s server certificate against a list of trusted certificate authorities. After this authentication, the client and SSL Relay negotiate requests in encrypted form. The SSL Relay decrypts the requests and passes them to the MetaFrame XP server.

When returning the information to the client, the MetaFrame XP server sends all information through the SSL Relay, which encrypts the data and forwards it to the client to be decrypted. Message integrity checks verify that each communication has not been tampered with.

For more information about configuring SSL Relay, see “Setting up Citrix SSL Relay” on page 162.

**Overview - Deploying the Secure Gateway for MetaFrame**

Using the Secure Gateway provides the following benefits:

- Removes the need to publish the addresses of every MetaFrame XP server
- Simplifies server certificate management
- Allows a single point of encryption and access to the MetaFrame XP servers

Use the Secure Gateway to create a gateway that is separate from the MetaFrame XP servers. Establishing the gateway simplifies firewall traversal because ICA traffic is routed through a widely accepted port for passage in and out of firewalls. The Secure Gateway provides increased scalability.

However, because ICA communication is encrypted only between the ICA Client and the gateway, you may want to use ICA Encryption to secure the traffic between the gateway and the MetaFrame XP servers.
For more information about implementing and configuring the Secure Gateway for MetaFrame, see the *Secure Gateway Administrator’s Guide* on the MetaFrame XP Components CD.

**Overview - Deploying ICA Encryption**

Unlike SSL/TLS encryption, ICA Encryption, used on its own, does not provide authentication of the MetaFrame XP server. Therefore information could, in theory, be intercepted as it crosses a public network and then be rerouted to a counterfeit server. Also, ICA Encryption does not provide integrity checking. Using ICA Encryption should be viewed as only one aspect of a comprehensive security policy.

Select the ICA Encryption level for a published application on the application’s **Properties** page.

You must also enable ICA Encryption for the ICA Client. See the documentation for the ICA Client you plan to deploy.

**Setting up Citrix SSL Relay**

The Citrix SSL Relay can secure communications between ICA Clients, servers running the Web Interface for MetaFrame XP, and servers running MetaFrame XP Server using Secure Sockets Layer (SSL) or Transport Layer Security (TLS).

The following sections cover:

- How to deploy SSL Relay in your MetaFrame XP farm.
- How to upgrade from a Feature Release 1 SSL Relay deployment. For more information, see “Upgrading SSL Relay from Feature Release 1” on page 168.

**Deploying MetaFrame with SSL Relay**

You must complete the following tasks to successfully deploy SSL Relay. More information about these tasks is included later in this chapter.

1. Obtain a server certificate for each MetaFrame XP server. A separate server certificate is needed for each MetaFrame XP server on which you use the Citrix SSL Relay.
2. Install the server certificate on each MetaFrame XP server.
3. Change the SSL Relay port number, if necessary. To use the SSL Relay and Internet Information Services (IIS) on the same server, you must change the port number used by IIS or the SSL Relay. See “Step 3 - Changing the SSL Port” on page 166.
4. In the SSL Relay, select the server certificate and allowed ciphersuites, according to your security policy. Change the target address or port, or add additional addresses for redundancy. For instructions, see “Step 4 - Configuring SSL Relay” on page 167 or the application online Help for the SSL Relay Configuration tool.

**Step 1 - Obtaining Root and Server Certificates**

Your organization’s security expert should have a procedure for obtaining certificates. Certificates must be signed by a trusted entity called a Certificate Authority (CA). Where you choose to obtain certificates depends on a number of factors, including:

- Whether or not your organization is a CA
- Whether or not your organization has already established a business relationship with a public CA
- The fact that the Windows operating system includes support for many public Certificate Authorities
- The cost of certificates and the reputation of a particular public CA

From your chosen Certificate Authority, you need to obtain a separate server certificate for each MetaFrame XP server on which you use the Citrix SSL Relay. The server certificate identifies a specific machine, so you will need to know the fully qualified domain name (FQDN) of each MetaFrame XP server.

You also need to install a root certificate on each client device. Root certificates are available from the same CAs that issue server certificates. The Web Interface for MetaFrame XP and the Citrix ICA Clients include native support for the following certificate authorities:

- VeriSign, Inc., http://www.verisign.com

This means that if you use server certificates from these certificate authorities, you won’t need to install a root certificate on your client devices. If you use a different certificate authority, you need to install root certificates and server certificates. See the documentation for the ICA Clients you are using for instructions about installing a root certificate.

**Requesting a Certificate**

After you decide on your Certificate Authority, you generate a request for a certificate using your Web server software. This generates information known as a **certificate signing request** (CSR) that you send to the Certificate Authority for signing.
You submit the CSR to the Certificate Authority, and then receive your signed SSL certificate and password in return. If your organization is a Certificate Authority, you should have your own procedures for supplying signed certificates.

**Important** The common name for the certificate must be the fully qualified domain name of the server.

You can use the Microsoft Web Server Certificate wizard in the IIS snap-in to request and import a certificate. You can use the wizard to request a certificate if you are using an external CA, or request and also install the certificate if you are using the wizard and using an online CA; for example, you have a Microsoft Enterprise Certificate Services set up.

To request a certificate using IIS

1. Click Start > Programs > Administrative Tools > Internet Services Manager.
2. In the Internet Information Services console, right-click Default Web Site and select Properties.
4. Select Create a New Certificate and then click Next.
5. Select Prepare the request now, but send it later and then click Next.
6. In the Name field, type the name for the server certificate. The Name field does not require that you enter the FQDN of the server; you can enter a server name.
7. In Bit Length, enter the bit length to be used for the certificate’s encryption strength. The greater the bit length, the higher the security. Citrix recommends that you select 1024 or higher. If you are specifying a bit length higher than 1024, verify that the ICA Clients you use can support it. Click Next.
8. Enter details about your organization. Click Next.
9. In Common Name, type the FQDN of the MetaFrame server on which the SSL Relay is running. Click Next.
10. Fill in the relevant geographical information. Click Next.
11. Save the certificate request and click Next. Verify the information in the Request File Summary. Click Next and then click Finish.

The information in the request can be sent to any CA for signing.
Step 2 - Installing the Certificate

The versions of SSL relay included with MetaFrame XP with Feature Release 2 and later use Microsoft’s own SSL implementation, known as SChannel. This means that SSL Relay uses the same registry-based certificate store as IIS, so you can install certificates using IIS or the Microsoft Management Console (MMC) Certificate Snap-in.

If you requested a certificate, when you receive a response from the CA, you can restart the Web Server Certificate wizard in IIS and the wizard will install the certificate. See the instructions in “Requesting a Certificate” for information about how to start the Web Server Certificate wizard. Alternatively, you can view and import certificates on the computer using the MMC.

To use the Microsoft Management Console (MMC) to import a certificate

1. Launch the Microsoft Management Console by choosing Start > Run and then typing mmc. Click OK.

2. If you do not see a Console Root folder, you must add the Certificates Snap-in.
   • From the Console menu, choose Add/Remove Snap-in. The Add/Remove Snap-in dialog box appears.
   • Click Add. The Add Standalone Snap-in dialog box appears.
   • Select Certificates and click Add. The Certificates snap-in dialog box appears.
   • Click Computer account and then click Next. The Select Computer dialog box appears.
   • Verify that Local computer is selected and then click Finish.
   • Click Close to close the Add Standalone Snap-in dialog box.
   • Click OK to close the Add/Remove Snap-in dialog box.

3. In the left pane of the console, click the plus sign (+) for Certificates (Local Computer) to expand the folder.

4. In the left pane of the console, click the plus sign (+) for Personal and then click Certificates.

5. In the right pane of the console, right-click the certificate to import, select All Tasks, and then click Import. The Certificate Import wizard appears.

6. Click Next and then click Browse to search for the certificate file to be imported.

7. Select the certificate file and click Next.
8. Enter the private key password in the Password box and click Next.
9. Click Next to accept the default values in the next window and then click Finish to import the certificate.

**Step 3 - Changing the SSL Port**

The Citrix SSL Relay uses TCP port 443, the standard port for SSL connections. Most firewalls open this port by default. You can optionally configure the SSL Relay to use another port. Be sure that the port you choose is open on any firewalls between the client devices and the MetaFrame XP server running the SSL Relay.

---

**Important** Microsoft Internet Information Services (IIS) Version 5.0 is installed by default on Windows servers and allocates port 443 for SSL connections. To run MetaFrame XP on a server running Windows 2000 or Windows Server 2003, you must configure IIS to use a different port or configure the SSL Relay to use a different port. You must install a server certificate on IIS before you change the port number. The following procedure includes instructions for adding a server certificate to IIS. You can use the same server certificate with IIS and the SSL Relay.

---

**To change the SSL port for Internet Information Services Version 5.0**

1. Run Internet Services Manager.
2. Click the plus sign (+) next to the Web site in the left pane.
3. Right-click Default Web Site and choose Properties. The Default Web Site Properties dialog box appears.
4. Select the Directory Security tab and click Server Certificate. The Welcome to the Web Server Certificate wizard appears. Follow the instructions in the wizard to create or import a certificate.
5. When your server certificate is installed, select the Web Site tab in the Default Web Site Properties dialog box.
6. Change the SSL port number to something other than 443.
7. Click OK to close the Default Web Site Properties dialog box.

**To change the Citrix SSL Relay port number**

1. Choose Start > Programs > Citrix > MetaFrame XP > Citrix SSL Relay Configuration Tool to run the SSL Relay configuration utility.
2. On the Connection tab, type the new port number in the Relay Listening Port box.
3. Click OK.
See the Web Interface Administrator’s Guide for the procedure to reconfigure servers running the Web Interface for MetaFrame XP with the new port number.

- **To run SSL Relay on port 443 without using HTTPS**
  1. Stop the Microsoft Internet Information Service.
  2. Configure and start the SSL Relay service.
  3. Restart the Microsoft Internet Information Service.

SSL Relay will use port 443 before IIS, including when the server is restarted.

**Note** When you install MetaFrame XP, members of the User group are allowed to edit registry entries in the registry hive HKEY_LOCAL_MACHINE\SOFTWARE\Secure\Citrix\Citrix SSL Relay.

You can use the Microsoft Security Configuration and Analysis tool to prevent members of the User group from editing these registry entries.

**Important** If you change the default Citrix SSL Relay port, you must set SSLProxyHost to the new port number in the ICA Win32 Client’s Appsrv.ini file. For more information about client settings, see the *ICA Win32 Client Administrator’s Guide*.

### Step 4 - Configuring SSL Relay

- **To configure the SSL Relay**
  1. On the MetaFrame server, click the **Citrix SSL Relay Configuration Tool** button on the ICA Administrator toolbar to start the SSL Relay configuration tool.
  2. On the **Relay Credentials** tab, select the server certificate.
  3. On the **Connection** tab, configure the address and port combinations to which the SSL Relay forwards decrypted data. The SSL Relay forwards packets only to the servers and ports listed on this tab.
  4. On the **Ciphersuites** tab, select which ciphersuites to allow.

For more information, see the Online Help for the SSL Relay Configuration tool.
Upgrading SSL Relay from Feature Release 1

The version of SSL Relay that shipped with Feature Releases 1 uses a different location for certificates and also supports certificates in PEM format that are not supported for use with the Microsoft Certificate Store.

To upgrade to Feature Release 2 or later, you need to convert any certificates from PEM format if necessary, and import the certificates from the original SSL Relay certificate folder (`keystore/certs`) into the Microsoft certificate store.

If you already set up SSL Relay for use on MetaFrame XP with Feature Release 1, follow these steps when you upgrade to Feature Release 2 or later:

1. Upgrade the MetaFrame XP server to the latest feature release. Upgrading does not automatically migrate the certificate, but does preserve the certificate in the `<WINNT>SSL Relay\keystore\certs` directory.

2. If your certificates are in PEM format, use the PEMtoPfx utility to convert them to Pfx format. To do this:
   
   At the command prompt, type:

   **pemtopfx <pem cert path>**

   The PEMtoPfx utility creates a new Pfx-formatted certificate file that you can import into the Microsoft Certificate store.

   **Important** It is technically possible to import a PEM-formatted certificate directly into the Microsoft certificate store; however, this does not maintain the private key and invalidates the certificate for use with the SSL Relay.

3. Use MMC to import the certificate into the Microsoft certificate store. See “To use the Microsoft Management Console (MMC) to import a certificate” on page 165 for more details.
Configuring MetaFrame XP Servers and Farms

This chapter describes options and settings for MetaFrame XP servers and server farms. It includes basic information about tools and utilities you use to manage servers and server farms. For more detailed information, see the online Help for the MetaFrame XP management tools, such as the Management Console for MetaFrame XP.

Some configuration options are part of MetaFrame XP Setup. For more information, see “Installing MetaFrame XP” on page 105.

Management Tools for MetaFrame XP

Citrix provides a comprehensive suite of utilities for managing MetaFrame XP servers, server farms, and ICA Clients. MetaFrame XP includes the Management Console for MetaFrame XP and additional tools, including utilities that let you manage MetaFrame 1.8 servers when your organization uses both MetaFrame 1.8 and MetaFrame XP.

This section provides an overview of the features and operations of MetaFrame XP tools. MetaFrame XP Setup installs the Management Console and other tools on the MetaFrame XP server by default when you install MetaFrame XP.

Note the Management Console can be installed on 32-bit Windows workstations (Windows NT, Windows 2000, or Windows XP) from the MetaFrame XP CD-ROM. Browse the Autorun screens to the Management Console for MetaFrame XP option.

If you are installing the console on a Windows NT 4.0 workstation, you may need to install the latest version of the Windows Installer, available from the Microsoft Web site.
Overview of MetaFrame XP Management Tools

Use the following tools to manage MetaFrame XP server farms. For more detailed information about each management tool, including the Management Console for MetaFrame XP, see the management tool's online Help.

Citrix Connection Configuration. Use this utility to configure the connections that ICA Clients use to link to MetaFrame XP servers. For information, refer to the online help in Citrix Connection Configuration and see “Configuring ICA Connections” on page 195.

Citrix Web Console. Citrix Web Console lets you monitor MetaFrame XP server farms from a supported Web browser. You can view server farm information and manage sessions with the Web console. For more information, see “Citrix Web Console” on page 181 and the online help available for the console.

Citrix SSL Relay Configuration. Use this utility to secure communication between an NFuse-enabled Web server and your MetaFrame XP server farm. For information, see “Setting up Citrix SSL Relay” on page 162.

ICA Client Creator. Use this utility to create diskettes or disk images for installing ICA Client software. For information, see “Deploying ICA Clients Using Diskettes” on page 227.

Note: ICA Client Creator is not supported on servers running Windows Server 2003.

ICA Client Update Configuration. Use this tool to manage the Client Update Database on a MetaFrame XP server. The database contains current ICA Client software for each supported client platform and can be used to install ICA Clients when users log on to the server. For information, see “Deploying ICA Clients to Users” on page 219.

Management Console for MetaFrame XP. Use this centralized administration tool to monitor and manage many aspects of MetaFrame XP operation from single servers to multiple server farms. For information, see “The Management Console for MetaFrame XP” on page 173.

Shadow Taskbar. Shadowing allows users to view and control other users’ ICA Client sessions remotely. You can use the Shadow Taskbar to shadow sessions and to switch among multiple shadowed sessions. You can also use the Management Console to shadow ICA sessions. For information about shadowing, see “Shadowing ICA Sessions” on page 284.
SpeedScreen Latency Reduction Manager. Use this tool to configure local text echo and other features that improve the user experience on slow networks. For information, see “Configuring Latency Reduction for ICA Clients” on page 192.

Using MetaFrame XP Tools and Utilities

As with other Windows programs, you can use several methods to run the management tools installed with MetaFrame XP. The most common method is to choose a shortcut from the Start menu on the MetaFrame XP server console.

- Shortcuts to launch MetaFrame XP management tools are in the Programs > Citrix > MetaFrame XP submenu on the Start menu.
- Shortcuts for the Management Console and Citrix documentation are in the Programs > Citrix submenu on the Start menu.
- The ICA Administrator Toolbar displays a series of buttons you can click to launch Citrix management tools and utilities. See “The ICA Administrator Toolbar” below.

The ICA Administrator Toolbar

The ICA Administrator Toolbar is a configurable desktop toolbar. You can use the toolbar to launch MetaFrame XP management tools and other programs.

After you install MetaFrame XP and restart the system, the ICA Administrator Toolbar appears at the right edge of the screen. The default configuration of the toolbar provides a button to run each MetaFrame XP management utility.

To run a utility program from the toolbar, click the program’s button on the toolbar.

You can reposition the ICA Administrator Toolbar by dragging it away from the right edge of the screen. If you drop the toolbar on the desktop, it becomes a floating toolbar. If you want the toolbar to snap to the edge of the screen, drag it close to the edge and then drop it (release the mouse button) when an outline of the toolbar appears along the edge of the screen.

Note A button for the Management Console appears on the ICA Administrator Toolbar if you install the console at the same time you install MetaFrame XP on a server. If you install the console later, the button does not appear, but you can add it to the toolbar as described in this section.
To display the Administrator Toolbar

When the toolbar is not displayed, you can make it appear by choosing **Start > Programs > Citrix > MetaFrame XP > ICA Administrator Toolbar**.

Configuring the ICA Administrator Toolbar

You can adjust the ICA Administrator Toolbar in the same ways you can adjust other toolbars in Windows. For example, you can drag the edge of the toolbar to make the toolbar larger or smaller.

You can right-click the toolbar to display a toolbar menu.

The menu contains commands that you can choose to change the behavior of the toolbar:

- **Autohide.** Choose **Autohide** to make the toolbar hide itself except when you point to it (move the mouse pointer to the screen edge where the toolbar is attached). This option has no effect if the toolbar is floating on the desktop. To turn off the Autohide option so the toolbar is always visible, choose **Autohide** again.

- **Always On Top.** This option makes the ICA Administrator Toolbar always appear in front of other windows and objects on the screen when it is displayed. When **Always On Top** is not selected, windows and other objects can appear in front of the toolbar when it is at the edge of the screen or floating.

- **Customize.** Choose **Customize** if you want to add or remove buttons from the ICA Administrator Toolbar. See the next section for more information about using Customize.

- **Exit.** Choose **Exit** to remove the toolbar from the screen. A dialog box asks if you want to display the toolbar again when you start MetaFrame XP. Click **Yes** if you want to display the toolbar when MetaFrame XP starts. Click **No** if you do not want to display the toolbar again.

Customizing the ICA Administrator Toolbar

You can use the Customize command in the ICA Toolbar menu to change the buttons displayed on the toolbar.

To customize the toolbar

1. Right-click the ICA Administrator Toolbar and choose **Customize** from the pop-up menu.
2. In the dialog box that appears, use the following options to customize the toolbar:
To hide a button on the toolbar, clear its check box in the list labeled *Show these files as buttons.*

To place a new button on the toolbar, click **Add Files**. Select the file you want to place on the toolbar and click **Add**. You can select any type of file, including executable files, help files, and text files.

To change the order of buttons, select a button name in the list. Then, click the arrow button above or below the word **Move**.

To remove an item from the list, select its name and click **Delete**. You can delete buttons and spaces that you add to the toolbar.

To change the name of a button, select it in the list and click **Rename**. Then type the new name in the dialog box and click **OK**.

To add space between buttons, select an item in the list and click **Add Space**. A space appears above the selected item in the list.

To restore the default button arrangement, click **Use Default**.

3. When you finish making changes, click **OK** to update the toolbar.

The Management Console for MetaFrame XP

The Management Console is the central console program that you use to monitor and manage MetaFrame XP server farms. The Management Console is a Java-based, extensible program that ships with MetaFrame XP.

The features and capabilities of the console depend on the MetaFrame XP family level installed and licensed in a server farm. The commands, controls, and features that you see in the console can vary from the descriptions and illustrations in this manual, depending on the components you install.

Installation Manager, Load Manager, Resource Manager, and Network Manager are optional components that are installed with MetaFrame XPe. When these components are installed and activated with a MetaFrame XPe license, additional features and functions are added to the Management Console.

MetaFrame XP Setup installs the console on each MetaFrame XP server by default. You can also use the MetaFrame XP CD-ROM to install the console on other workstations that you want to use to manage MetaFrame XP server farms.

In a MetaFrame XP server farm, use the Management Console to:

- Configure server and farm settings
- Create MetaFrame XP administrator accounts and assign access to tasks
- Create policies for users or user groups
- View information about current sessions, users, and processes
Set up and manage printers for ICA Client users
- Publish applications and monitor application usage
- Enter, activate, and assign MetaFrame XP licenses
- Monitor, reset, disconnect, and reconnect ICA Client sessions
- Send messages to users and shadow their ICA sessions

**Note**  Scrolling with the Microsoft wheel mouse is not supported in the Management Console.

To use the Management Console, you must be a MetaFrame XP administrator. Administrators can have varying levels of access to areas of MetaFrame XP farm management. For example, you can be a MetaFrame XP administrator but have view-only access or even no access to some areas of MetaFrame XP administration. If you try to access an area of the console that you are not authorized to use, the right pane of the console may be blank.

**Configuring MetaFrame XP Administrator Accounts**

When you create a MetaFrame XP administrator account, you can select individual user accounts and group accounts from Windows and NDS account authorities. For information about management of Windows domains and user accounts, refer to your Windows system documentation or online help. For information about enabling NDS accounts in server farms, see “Supporting Novell Directory Service Users” on page 72.

**Tip**  Use your standard network administrators group to add MetaFrame XP administrator accounts to the console, so administrators have access to manage network resources including print servers.

MetaFrame XP administrators manage MetaFrame XP server farms. You can create MetaFrame XP administrators accounts with the following permission levels:
- Full access to all areas of MetaFrame XP server farm management.
- View-only access to all areas of server farm management.
- Access to areas of farm management or specific tasks within those areas; administrators can have a mixture of view-only access, write access, or no access.
Important If you try to access an area of the console that you are not authorized to use, the right pane of the console may be blank.

Restricting access to areas of farm management may not prevent administrators from running some MetaFrame XP command-line utilities.

To take full advantage of new features, Citrix recommends that you do not mix releases of MetaFrame XP in the same server farm. For example, do not run Feature Release 2 on some servers in the server farm and Feature Release 3 on other servers in the same farm.

If you use a version of the Management Console released prior to MetaFrame XP with Feature Release 3 to connect to a MetaFrame XP server running a version of MetaFrame XP released prior to Feature Release 3, custom settings applied to MetaFrame XP administrators accounts are not recognized.

During MetaFrame XP setup, you must enter credentials for a primary MetaFrame XP administrator. If you are installing the first MetaFrame XP server in a new server farm, the user account that you specify becomes the first MetaFrame XP administrator for the new server farm. This administrator account has full access to all areas of MetaFrame XP. You must log on to the Management Console with this account to add other users to the MetaFrame XP Administrators group.

Note One MetaFrame XP administrator account that has full access must always exist in the server farm. Therefore, no administrator can delete the last full access administrator account from the MetaFrame XP Administrators group.

Creating Customized MetaFrame XP Administrators

You can delegate areas of MetaFrame XP administration and farm management to your IT staff. You can create specialized MetaFrame XP administrators and allow them to perform specific administration tasks such as managing printers, published applications, or user policies. MetaFrame XP administrators can carry out their assigned tasks without being granted full access to all areas of farm management.

The level of permission to grant for various areas of farm management depends on the specific business function of the administrator. For example, your system or network administrators may need complete access to all areas of farm and server management, while help desk personnel may need view-only access to most areas. You can also grant access to MetaFrame XP features and functions without granting access to the Management Console.
To add users to the MetaFrame XP Administrator group, a MetaFrame XP administrator with full access logs on to the Management Console and creates other administrator accounts.

**Important** If you recreate the server farm’s data store database, a MetaFrame XP administrator account with full administration rights is created using the local administrator account credentials. Be sure to create a new administrator with full administration rights in the Management Console. Doing so replaces the default MetaFrame XP administrator account that uses the local administrator credentials. Be sure to back up any database before you attempt to recreate it.

### To create MetaFrame XP administrator accounts and assign tasks

1. Right-click the MetaFrame XP Administrators node in the left pane of the console and choose **Add MetaFrame XP Administrator**. The first page of the Add MetaFrame XP Administrator wizard appears.

   **Tip** You can click the New MetaFrame XP Administrator button on the toolbar or choose **Actions > New > MetaFrame XP Administrator** to add accounts to the MetaFrame XP Administrators group.

2. Select the user or group accounts that you want to add to the MetaFrame XP Administrators group and then click **Add**.
   Click **Add List of Names** to enter user names in a separate dialog box. Select **Show Users** to display all user names in the selected domain.

3. Click **Next** after you add the users or groups to the list of configured accounts. The second and final page of the Add MetaFrame XP Administrators wizard appears.

4. Select the level of permission you want this administrator account to have.
   Select **View Only** to allow view-only access to all areas of MetaFrame XP administration. Select **Full Administration** to allow full access to all areas.

5. To grant access to only some areas of MetaFrame XP administration, select the areas or specific tasks within an area you want the administrator to be able to access.
   For example, you can create one MetaFrame XP administrator account that has full access to all printer management tasks, but view-only access to published application information.
Important You can deny access to the Management Console by expanding the MetaFrame XP Administrators node and clearing the check mark from the Log on to the Management Console for MetaFrame XP task. This capability is allowed by default for all new MetaFrame XP administrator accounts.

Using the Management Console for MetaFrame XP

To use the Management Console, you must be an authorized user whose Windows user account is included in the MetaFrame XP Administrators group in the console. To run the console, you must enter your user name, password, and network domain.

To log on to a MetaFrame XP server farm with the console, specify any MetaFrame XP server in the server farm. The console connects to the server and then displays information for the entire server farm and for the individual servers in the farm.

In the Log On dialog box for the console, the name of the last server that the console connected to appears in the Citrix MetaFrame XP Server box. The drop-down menu displays the names of other servers that the console connected to recently.

Important You can use the Management Console to monitor and manage MetaFrame XP server farms. However, you cannot use the console to manage MetaFrame 1.8 server farms. When MetaFrame XP servers are set to interoperate with MetaFrame 1.8 servers, the console displays information about MetaFrame XP server farms only.

To use the Management Console

1. From the Start menu, choose Programs > Citrix > Citrix Management Console, or click the corresponding button on the ICA Administrator Toolbar.
2. When the console starts, a dialog box asks you to log on to a MetaFrame XP server.
   - In the Citrix MetaFrame XP Server box, enter the name of a MetaFrame XP server in the server farm, or select a server from the drop-down menu. You can connect to any server in a farm to manage the entire farm.
   - Type your user name, domain, and password for your Windows user account. The account must be in the MetaFrame XP Administrators group in the console.
3. Click OK.
Tip
You can click the Management Console button on the ICA Administrator’s toolbar to launch the console.

Switching Server Farms and Logging Off

When you are using the console and you want to log on to a different MetaFrame XP server farm, choose Actions > Log Off from Citrix MetaFrame XP Server Farm. The Log On dialog box appears and you can specify another MetaFrame XP server to log on to. You also use the Log Off from Citrix MetaFrame XP Server Farm command to exit the console if you do not want to keep the console running.

Using Online Help in the Management Console

For detailed information about using the Management Console, refer to online Help in the console.

- To view online help in the Management Console

  When the Management Console is running, choose Help > Contents and Index. The online help system provides detailed information about terms, concepts, and procedures related to management of MetaFrame XP server farms.

Data Displayed in the Management Console

When you are connected to a MetaFrame XP server farm, the Management Console displays a window with two main parts, called panes.

- The left pane shows a hierarchical list of the components of a Citrix server farm.
- The right pane displays information about the object selected in the left pane.
Several common terms are used in this and other Citrix documentation to refer to the items you see in the Management Console window.

**The Tree View**

The list of items in the left pane is referred to as a tree, because the pane displays the server farm as a hierarchy with objects that branch off from a root object. The tree view is similar to the tree view in Windows Explorer and Microsoft Management Console.

The object at the top of the tree in the Management Console for MetaFrame XP represents a MetaFrame XP server farm. The next level of objects under the server farm represent management features and components in the server farm. These objects are called nodes. In a MetaFrame XP environment, the nodes represent areas such as Applications, Printer Management, Licenses, and Servers.

Objects that appear under the nodes in the console tree view represent specific features and items in the server farm. For example, individual published applications appear under the Applications node and individual MetaFrame XP servers appear under the Servers node.

The function of the console tree is similar to the Windows Explorer tree.

- A plus symbol (+) indicates that a branch of the tree is compressed. Click the symbol or select the node and press the right-arrow key to expand the branch.
- A minus symbol (-) indicates that a branch is expanded. Click the minus symbol or select the node and press the left-arrow key to compress the branch and hide the objects under the node.

When an object is selected, the object appears highlighted in the tree. To select another object, you can click the object or use the arrow keys to move the highlight.

You cannot select multiple objects in the console tree. However, you can select multiple objects on the Contents tab in the right pane by pressing CTRL and clicking each object or pressing Shift and clicking to select a contiguous range of objects.

**Tab Views**

The right pane of the console displays one or more screens, which are called tabs because each screen has a tab-shaped label at the top. The tab or tabs that are available in the right pane are based on the node or object that is selected in the tree.

The name of the tab appears at the top of each tab. One tab at a time is selected in the right pane, and the contents of one tab appear in the right pane. To use a different tab, click its name.
In most cases, a **Contents** tab appears in the right pane when you select a node in the tree. The **Contents** tab displays the objects that are under the selected node. You can double-click an object on the **Contents** tab to open the object; this action has the same effect as expanding a branch and selecting an individual object such as a published application or a MetaFrame XP server in the tree.

**Controlling Refresh of Data in the Console**

To reduce network traffic and improve responsiveness, the Management Console does not refresh all data automatically. In general, the console receives notifications of events as they occur on MetaFrame XP servers and updates the displayed data in response to these events. However, some changes you make in the console and some events, such as a server coming online in the farm or an ICA session starting, does not cause the console to update the displayed data.

You can enable automatic data refresh so that the console automatically updates the display at a fixed rate. When you enable automatic refresh, you can specify the refresh rate. Whether automatic refresh is enabled or not, you can refresh the console’s display manually at any time.

Refresh the console display when you view license usage data. Even if automatic refresh is enabled, the display of license usage data might not be current until you perform a manual refresh. When you view data about ICA sessions and servers, it is also useful to refresh the display manually to be sure that you view current information.

- **To manually refresh the data displayed in the Management Console**
  
  Choose **View > Refresh <farm_name>** or press F5. The Refresh command updates the information that appears on the current tab and tree view.

- **To enable automatic refreshing of data in the Management Console**

  You can use the Management Console to automatically refresh data for servers, server folders, applications, and licensing.

  1. Choose **Preferences** from the **View** menu.
  2. Select **User Data** to choose options to automatically refresh data for servers, server folders, and applications. After you choose an option, you can set the refresh rate. Enter the time in seconds to set the rate at which automatic refreshing occurs.
  3. Select **License Data** to enable automatic refreshing of licensing data and enter the time in seconds to set the refresh rate.
  4. Click **OK** to apply the refresh settings to the console.
Citrix Web Console

Citrix Web Console lets you monitor MetaFrame XP server farms by using a Web browser. You can view information about a server farm, including its active sessions, published applications, servers, and users.

With the Web console, you can also manage sessions by logging off sessions, shadowing sessions, disconnecting sessions, and sending messages to users, the same as you would with the Management Console.

You can use the MetaFrame XP CD to install the Web console on MetaFrame XP servers or on servers not running MetaFrame XP. From the Autorun screen, browse to the option to install the Web console.

The Web console server must be in the same security context as the MetaFrame server. Local accounts work only if the Web console server is also acting as a MetaFrame server. You cannot use Novell Directory Services (NDS) accounts with the Web console.

For more information about using the Citrix Web Console on a computer that is not running MetaFrame XP, see Advanced Concepts for MetaFrame XP, available from the Citrix Web site. This document is revised for each new feature release, so be sure to read the latest version.

Citrix Web Console supports Microsoft Internet Explorer 4.0 and later Web browsers.

To use Citrix Web Console, the server must have Microsoft Internet Information Services (IIS) 5.0 (or later) installed.

**Important** Citrix Web Console does not encrypt information that it sends to Web browsers. When a user logs on to the console, the user’s MetaFrame XP administrator credentials are sent to the Web console as unencrypted text. For maximum security, configure your Web browser and IIS to use SSL encryption. For information about setting up SSL communication, refer to the documentation for IIS and your Web browser.

After you install the Web console, the default URL for accessing the console is http://hostname/Citrix/WebConsole, where hostname is the name of the MetaFrame XP server on which the Web console is installed.

When you browse to the URL for the Web console, a logon dialog box appears. Enter your MetaFrame XP administrator user name and password to log on to the console. If the MetaFrame XP administrator account is not a local administrator account on the host server, you must enter the domain and user name in the **User Name** box, as follows:

domain/username
For more information about using the Web console, log on to the console and click Help.

**Configuring MetaFrame XP Properties**

Configuring options and settings for MetaFrame XP servers and server farms takes place in two stages. First, you set options when you install MetaFrame XP on the first server in a server farm and on other servers that you add to the farm. Then, as the server farm is operating, you can adjust settings on individual servers and set options for the server farm using the Management Console.

**Setup options.** Some configuration options are available only during MetaFrame XP setup. For example, you choose the name of a server farm when you install MetaFrame XP on the first server in the farm. If you set restrictions on ICA shadowing during setup, the restrictions are permanent on the MetaFrame XP server. For details about setup options for MetaFrame XP servers and server farms, see “Installing MetaFrame XP” on page 105.

**Operating options.** After you create a MetaFrame XP server farm, you can use the Management Console to change settings such as ICA display options and to manage ICA sessions on individual servers. You also use the console to configure options that affect performance, zone configuration, and interoperation with MetaFrame 1.8 servers for the entire server farm.

**Properties of MetaFrame XP Server Farms**

After you log on to a server in the farm with the Management Console, the console title bar displays the name of the server farm. In the left pane of the console, the farm name is the label of the main node at the top of the tree.

This section describes ways to manage farm configuration after you install MetaFrame XP. For options you can configure only during MetaFrame XP setup, see “Installing MetaFrame XP” on page 105.

MetaFrame XP also includes some commands that you can run from the command prompt to monitor and configure servers. For information about these commands, see “MetaFrame XP Commands” on page 311.

**Using the Farm Properties Page**

To configure MetaFrame XP server farm properties, log on to the console and select the server farm node in the console tree. The server farm is represented by the first node, at the top of the tree in the left pane of the console. The label of the server farm node is the name of the server farm.
Most configuration options and settings for a MetaFrame XP server farm are available in the farm’s Properties page in the Management Console. When you configure farm settings, the settings apply to the entire farm, including servers that are temporarily offline.

To display the Properties page for the server farm, select the farm node and choose Properties. The Properties command is available in the Actions menu, on the console toolbar, and from the menu that appears when you right-click the farm node.

To set options for the server farm, select the area that you want to configure from the left pane of the farm’s Properties page. All of the settings in the page apply to the entire farm. Some settings affect each MetaFrame XP server in the farm. Other settings apply to the farm’s data store that all servers in the farm use to store and retrieve farm configuration information.

When you make changes in the Properties page, the changes do not take effect until you click OK, which closes the page and applies all the current settings. If you click Cancel, the page closes and all changes you made in the page are discarded.

For information about specific options, click the Help button in the Properties page. Some general information about options that are available in the Properties page for both farms and servers is included in this chapter.

**ICA Display Options**

Use ICA Settings in the left pane of a farm’s Properties page to configure the transmission of display information and application graphics to clients.

You can optimize the display for ICA Clients by adjusting the amount of memory used for graphics and selecting other options that conserve bandwidth for ICA display transmission.

ICA uses highly optimized protocols to send the screen display of applications to ICA Client users. On standard (non-dialup) networks, the default settings are designed for optimum performance. You do not need to reconfigure ICA display settings under most circumstances. However, you can adjust these settings for better performance when many users dial in to your server farm, or users’ network access includes slow WAN links.

In the Resource Limits area, you can set a maximum amount of memory to be used on the MetaFrame XP servers for ICA display.

**Note** You can use ICA Settings and the TWCONFIG utility to set the maximum amount of memory used for an ICA session on the MetaFrame XP server. For more information about the TWCONFIG utility, see “MetaFrame XP Commands” on page 311.
You might want to set a memory limit that accommodates typical sessions but prevents excessive memory usage by sessions that specify extremely large display sizes, such as 32,000 by 32,000 pixels at 24 bits per pixel, for example. If a session exceeds the memory limit that you set, the server scales down the session to a lower resolution to accommodate the memory limit.

Set options that specify that the server reduce the session display size (resolution) or color depth on **ICA Settings**.

**Effects of Memory Limits on Seamless ICA Sessions**

When an ICA Client initiates a session in seamless mode, the size of the session is equivalent to a full-screen session. For example, a seamless session initiated by a client with a desktop size of 1,600 by 1,200 pixels, at 24 bits per pixel color depth, requires 5,760,000 bytes (5.5MB) of memory.

When a client device running Windows 98 or Windows 2000 has multiple monitors, the total desktop size is the total of both monitors, and the memory required for a seamless session is based on the total display size of both monitors.

If you set a memory limit that is less than that required for the display size and color depth, the server scales down the session. If the option to reduce the resolution of the session is selected on **ICA Settings**, the application launches in a remote desktop rather than a seamless mode window. If the option to reduce color depth is selected, the server might be able to accommodate a seamless mode session at a lower color depth.

**General MetaFrame XP Options**

Click **MetaFrame Settings** in the left pane of a farm’s **Properties** page to set options that control communication and other aspects of IMA, the Citrix protocol for communication among servers in your server farm. You also configure the way MetaFrame XP servers respond to broadcasts from ICA Clients in **MetaFrame Settings**.

**Setting up Response to ICA Client Broadcasts**

With the options in the Broadcast Response area on **MetaFrame Settings**, you can control whether or not the data collectors and RAS servers in your server farm respond to UDP broadcasts from ICA Clients.

You might want servers to respond to broadcasts if you have legacy ICA Clients that require this, or if all your ICA Clients use TCP/IP (rather than TCP/IP + HTTP) to auto-locate MetaFrame XP servers.
Select the option **Data Collectors respond to ICA Client broadcast (UDP) messages** if your ICA Clients do not have a specific server address designated for locating applications in the server farm and use TCP/IP protocol to auto-locate MetaFrame XP servers.

To use the UDP response option, you must also configure the MetaFrame XP server farm to interoperate with a server farm composed of MetaFrame 1.8 servers. To do this, select **Interoperability** from the left pane of the farm’s **Properties** page and select **Work with MetaFrame 1.8 Servers**. If you do not select this option and MetaFrame XP detects MetaFrame 1.8 ICA Browsers on the same network subnet, MetaFrame XP disables the broadcast response.

If you have ICA Client users who dial in to MetaFrame XP servers using RAS, select **RAS servers respond to ICA Client broadcast messages**. Because a dial-in client communicates only with the RAS server and cannot contact ICA Browsers or data collectors to locate the server farm’s published applications, this option lets the dial-in clients locate applications in the server farm.

**Important** If two server farms of MetaFrame XP servers are on the same subnet and both farms respond to ICA Client broadcasts, users will have problems browsing for published applications in the server farms.

---

### Content Redirection from Server to Client

You can use **MetaFrame Settings** in the left pane of the farm’s **Properties** page to enable Content Redirection from server to client for the entire server farm. When you enable Content Redirection from server to client, embedded URLs are intercepted on the MetaFrame XP server and sent to the ICA Client using the ICA Control virtual channel. The user’s locally installed browser is used to play the URL. Users cannot disable this feature. You can enable Content Redirection for the entire server farm or for selected servers.

### ICA Client Time Zones

If users connect to the server farm from different time zones, you can configure the farm to support the local time zones of client devices. Not all ICA Clients support this feature; see the **ICA Client Administrator’s Guides** for more information.

Local time zone support provides correct local date and time stamps on files created by clients.

To enable local time zone support, select the option in the Client Time Zones area. For ICA Clients that do not report their local time zone to MetaFrame XP servers, the local time is estimated. You can disable local time estimation if this option causes incorrect local time display in ICA Clients.
SNMP Trapping and License Notification Options

If you use an SNMP-based network management product, the MetaFrame XP SNMP Agent can send traps if the usage of MetaFrame XP licenses in the server farm exceeds thresholds that you specify.

You can use SNMP in the farm’s Properties page to select options to enable SNMP traps for individual servers or for the farm.

To enable SNMP notification messages on a farm-wide basis, select Enable SNMP Agent on SNMP in the Properties page.

In the Set box, enter the percentage of available pooled licenses (or of licenses assigned to a server) below which the SNMP Agent alerts the management product. The alert status remains in effect until the percentage of available pooled licenses (or of licenses assigned to a server) exceeds the value in the Reset box.

SNMP notification is available when you install the Citrix plug-ins for Tivoli NetView, HP OpenView, or CA Unicenter TNG network management consoles. For information about which SNMP management consoles you can use with Network Manager, see the documentation for Network Manager in the Docs directory on the MetaFrame XP CD-ROM.

Configuring MetaFrame XP Server Properties

In addition to settings for an entire farm, you can configure settings for individual MetaFrame XP servers in the farm through the Management Console. You can access most server configuration options from the Properties page for each server.

When you change settings for a server’s properties, the console applies the settings immediately if the server is available. If the server is offline or busy, the console applies the settings as soon as the server becomes available.

This section describes ways to manage server configuration after you install MetaFrame XP. For options you can configure only during MetaFrame XP setup, see “Installing MetaFrame XP” on page 105. MetaFrame XP also includes some commands you run from the command prompt to monitor and configure servers. For information about these commands, see “MetaFrame XP Commands” on page 311.

Using the Server Properties Page

To configure the settings of an individual server, select the server under the Servers node in the console tree. Then choose the Properties command from the Actions menu, the console toolbar, or by right-clicking the server. The Properties command displays the Properties page for the selected server. The settings that you configure in the Properties page apply to the selected server only.
For example, you can configure SNMP traps by selecting **SNMP** in a server’s **Properties** page. These SNMP settings apply to a single server. If you select the farm node and use the farm’s **Properties** dialog box, you can set SNMP settings that apply to all servers in the server farm.

**Note**  The Servers node in the console tree does not include a **Properties** page. When you want to apply settings to multiple servers, you use the Farm node or another node in the console tree.

Use a server’s **Properties** page to view and configure the following:

- **Published application information.** Use **Published Applications** in the left pane of the server’s **Properties** page to view the names, status, connection type, and other information about the applications that are published on a selected server.

- **SNMP traps.** You can use **SNMP** to enable the SNMP Agent and select the events that trigger SNMP messages on the selected server. For more information, see “SNMP Trapping and License Notification Options” on page 186.

- **Server and network information.** Use **Information** to display software, network, and licensing information for the selected server. **Information** displays the versions of Windows and MetaFrame XP software that are installed and the installation date. **Information** also displays the product code that is assigned to the server, which specifies the type of product license that the server uses. You can also verify that logons by ICA Client users are enabled and check the network address.

- **Product code.** Use **Information** to display the product code that is set on the selected server. The product code specifies the type of product license the server uses from the server farm’s license pool. You cannot use **Information** to change the product code. For more information about changing product codes and licensing, see “Product Codes” on page 143. You might want to change the product code if you purchase a product upgrade or a full retail license for a server that uses an evaluation license.

- **Installed hotfixes.** Use **Hotfixes** to view a list of hotfixes that are installed on the selected server. **Hotfixes** displays the name and installation date of each hotfix that is installed.

- **ICA Settings options.** You can use **ICA Settings** to affect graphics and video display on ICA Clients. These settings apply to the applications that run on the selected server. The options let you conserve bandwidth used to transmit graphics to ICA Clients and to specify the size of the memory buffer to use for graphics display. Use **ICA Settings** to configure auto client reconnection for the farm.
ICA Browser and logon settings. Use MetaFrame Settings to display various configuration settings for the selected server. You can set options in MetaFrame Settings that affect the selected server’s response to UDP broadcasts from ICA Clients. UDP broadcasts allow ICA Clients to browse for published applications in a server farm that includes ICA Browser-based MetaFrame servers. Other options let you control the logging of shadowing events on the server.

Citrix XML Service. Use MetaFrame Settings to display the port used by the Citrix XML service for TCP/IP+HTTP browsing by ICA Clients. You cannot edit the port used in MetaFrame Settings, but you can change the port by typing `ctxxmlss /r` at a command prompt, with the actual port number following `/r`. This configures the XML Service to auto start on port `xxxx`. To activate the new settings, you must stop and restart the service.

Content Redirection from Server to Client. Enable Content Redirection from server to client for the selected server using MetaFrame Settings. When you enable Content Redirection from server to client, embedded URLs are intercepted on the MetaFrame XP server and sent to the ICA Client using the ICA Control virtual channel. The user’s locally installed browser is used to play the URL. Users cannot disable this feature.

Controlling printer bandwidth. If you want to limit the bandwidth that MetaFrame XP uses for printing by clients, you can enter a value on Printer Bandwidth in the left pane of a server’s Properties page. To remove a bandwidth limit, select the Unlimited option. This setting applies to the selected server. You can view the current setting for each server on the Bandwidth tab when you select Printer Management in the console tree.

For more information about client printing and bandwidth, see “Bandwidth Tab” on page 297.

ICA Keep Alive. Enable ICA Keep Alives to manage the state of an ICA connection. For example, an ICA session on a broken connection can sometimes still appear active. When you enable ICA Keep-Alive, packets are sent to a client device to determine if a connection still exists. If a client device does not respond to the packets, the state of the session using the connection is changed from active to disconnected.

When the ICA connection is reestablished, users can reconnect to the session only if it is in a disconnected state. If users can reconnect to a disconnected session, they can resume working in the published application where they were interrupted.

SpeedScreen Browser Acceleration. Enable SpeedScreen Browser Acceleration to lower bandwidth consumption for users running HTML-capable applications published on MetaFrame XP servers. Users can click Back and Stop in the browser window and interact with elements on a page while the page downloads. Scrolling is similar to scrolling in a local browser.
Selecting Other Settings to Configure

To change some settings for individual servers, you use the Licenses, Printer Management, and Applications nodes in the the Management Console tree.

You can:

- Assign licenses to servers and monitor license usage from the Licenses node
- Publish applications on servers and monitor application usage through the Applications node
- View and replicate printer drivers installed on servers from the Printer Management node

Select individual MetaFrame XP servers to configure settings that are not associated with application publishing, printer management, or licensing.

Configuring Zones and Data Collectors

In a MetaFrame XP server farm, a zone is a grouping of MetaFrame XP servers that share a common data collector, which is a MetaFrame XP server that receives information from all the servers in the zone.

By default, all servers in a farm that are on the same network subnet belong to the same zone. Use Zones in the left pane of a farm’s Properties page to create and configure additional zones, to change the zones of MetaFrame XP servers, and to configure zone data collectors.

**Important** If you change a server’s zone membership (move the server to another zone), incorrect information can appear in the Management Console until the server updates the data collector. To ensure data synchronization, restart a MetaFrame XP server after you change its zone membership.

Zones are designed to enhance the performance of a MetaFrame XP server farm by allowing geographically related servers to be grouped together, whether they are connected to the same network subnet or not.

- If all the servers in a farm are in one location, you can configure the farm with a single zone without causing slower performance or making the farm more difficult to manage.
- If you manage an enterprise server farm with servers in different geographic regions, you can place servers in zones based on the location of the servers. This can improve performance and make management of the farm more efficient.
You can use **Zones** on a farm’s **Properties** page to view the servers that belong to each zone in the farm. You can create, delete, and rename zones. To change the membership of a server from one zone to another, select the server from the list of servers in the zone and then move the server to another zone.

**Functions of Data Collectors**

Each zone in a server farm contains one MetaFrame XP server that is designated as the data collector for the zone. Data collectors store information about the servers and published applications in the server farm. The data collector knows the addresses of each server and the applications that are available on each server in the zone.

**Note** Data collectors in IMA-based server farms are similar in function to ICA Browsers in MetaFrame 1.8 server farms. However, data collectors use TCP/IP for server-to-server communication. ICA Browsers use UDP for server-to-server communication.

Data collectors are communication gateways between zones in server farms that have more than one zone. Each data collector communicates with the other data collectors in other zones in the server farm.

Because data collectors serve as communication gateways among zones, every server in the farm does not need to communicate with every other server. Servers that are separated by long distance and slow communication links do not add communication traffic to the server farm. Only data collectors send messages between zones.
Tip Because of the way data collectors concentrate communication among the servers in a farm, use zones if you have a geographically diverse farm.

Election of Data Collectors

A zone in a MetaFrame XP server farm elects, or selects, a data collector for the zone if a new server joins the zone or the current data collector becomes unavailable. A data collector becomes unavailable if the server goes down, is disconnected from the network, or if you move the server to another zone.

When a zone elects a new data collector, it uses a preference ranking of the servers in the zone. You can set the preference ranking for the servers in a zone using Zones in the left pane of a server farm’s Properties page.

Each zone has four levels of preference for election of data collectors. The preference levels, in order from highest to lowest preference, are:

1. Most Preferred
2. Preferred
3. Default Preference
4. Not Preferred

All servers in a zone are assigned to one of the four election preference levels. When the zone elects a new data collector, it tries to select a server from the first preference level. If no servers are available at this level, the zone selects a server from the second level, and so on.

When you create a farm, the election preference for all servers is Default Preference, except for the first server added to the zone, which is set to Most Preferred and is the zone’s initial data collector.

If you select Zones on the left pane of a farm’s Properties page, a colored symbol appears next to each server name to indicate the election preference setting.

You can change the default election preference to designate a specific server as the data collector. To do this, set the election preference for the server to Most Preferred. If you do not want some servers to be data collectors, set the election preference for those servers to Not Preferred.

Assign servers that you do not want to become data collectors (except as a last resort) to the Not Preferred level.

Tip In large server farms and enterprise networks with high client traffic, you can reduce the possibility of data collector performance issues by using dedicated data collectors. You can do this by setting up data collectors on MetaFrame XP servers that do not host applications for client sessions.
Setting the Election Preference for Data Collectors

To change a server’s data collector election preference, select the server in the list, select Zones, and click Set Preference. In the dialog box, select the election preference level to assign to the server.

To designate a specific server to be a zone’s data collector when the next election occurs, make sure that the server has the highest election preference. You can do this by making the server the only one set to Most Preferred level, for example. The zone will elect the server to be the data collector when the next election occurs.

If you create a new zone, the first server that you move to the new zone becomes the zone’s data collector, and its preference level is set to Most Preferred.

Zones do not maintain backup data collectors. Instead, the data store for the entire MetaFrame XP server farm maintains information that is used by each data collector.

Configuring Latency Reduction for ICA Clients

Delays between entry and echo of mouse movements and keyboard input is one of the primary frustrations that users can experience on a high-latency network connection. SpeedScreen features in MetaFrame XP and the ICA Client software enable almost immediate echo of mouse movements and keystrokes at the ICA Client.

Use the SpeedScreen Latency Reduction Manager to customize SpeedScreen settings for a MetaFrame XP server, individual published applications, and input controls within applications. You can save a SpeedScreen configuration file and then deploy the file across your server farm.

To launch SpeedScreen Latency Reduction Manager, from the Start menu, choose Programs > Citrix > MetaFrame XP > SpeedScreen Latency Reduction Manager.

Tip You can launch SpeedScreen Latency Reduction Manager by clicking its button on the ICA Administrator Toolbar.

By default, instant mouse click feedback is enabled and local text echo is disabled for all applications.

You can enable local text echo on an application-by-application basis only. If you use this feature, the programs to which you apply it must use only standard Windows APIs for displaying text or the settings will not work correctly.
Important Test all aspects of an application with local text echo in a non-production environment before enabling text echo for your users.

With SpeedScreen Latency Reduction Manager, you can also configure local text echo settings for individual input fields within an application. See the application help for the SpeedScreen Latency Reduction Manager utility for more configuration information.

For general information about SpeedScreen options, see the online help in the SpeedScreen Latency Reduction Manager.

Deploying SpeedScreen Settings

After you use SpeedScreen Latency Reduction Manager to configure SpeedScreen settings for the server (and specific applications, if you want), the manager saves the settings for each application in the directory C:\WINNT\system32\ss3config. To deploy the configuration settings throughout a server farm, copy the entire directory and its contents to each MetaFrame XP server in the server farm.

Tip If you plan to copy SpeedScreen configuration settings across a server farm, apply the settings to all instances of an application on the server when you configure individual application settings, because path names might differ on various destination servers.

The SpeedScreen Latency Reduction Manager uses window names to identify exception entries, and could apply saved settings erroneously on a destination server if you apply SpeedScreen settings to a specific instance of the application.

Improving Responsiveness with SpeedScreen Browser Acceleration

SpeedScreen Browser Acceleration improves performance for users running Outlook, Outlook Express, or Internet Explorer 5.5 or higher as applications published on MetaFrame XP servers.

Enabling SpeedScreen Browser Acceleration lowers bandwidth consumption when users run these applications. Users can click Back and Stop in the browser window, and interact with elements of a page while the page downloads. Scrolling response in the browser is also improved.
Note Users must be running Version 7.0 of the ICA Win32 Client, with a minimum connection color depth of 16-bit, to realize the SpeedScreen Browser Acceleration improvements.

Users with limited bandwidth connections benefit the most from SpeedScreen Browser Acceleration. Users connecting within the LAN may see improvement only when networks are congested. Enabling SpeedScreen Browser Acceleration uses more resources on both servers and clients.

Note Enabling SpeedScreen Browser Acceleration results in slightly lower image resolution.

You can enable SpeedScreen Browser Acceleration from the Properties page for individual servers or for the entire server farm.
MetaFrame XP lets users run applications published on MetaFrame XP servers by enabling connections from varied computer platforms through ICA Client software. Managing the connections to your server farm involves management of network access and ICA connections to the farm.

You manage user access through standard Windows permissions and account configuration tools. MetaFrame XP provides the tools you use to configure ICA connections.

**Overview of ICA Connections and Sessions**

Users can access applications on a MetaFrame XP server through ICA connections and ICA sessions.

*ICA connections* are logical input/output ports that are set up on a MetaFrame XP server. When an ICA Client links to a MetaFrame XP server through an ICA connection, it establishes an ICA session. The *ICA session* is an active link that runs on the MetaFrame XP server until the user logs off and ends the session.

This section explains how ICA connections and ICA sessions work together. It includes information about using Citrix Connection Configuration to configure ICA connections. Later sections in this chapter tell you how to set properties for ICA sessions.

*Note* In addition to ICA connections, Citrix Connection Configuration supports connections using Microsoft’s RDP protocol for terminal services. ICA Client settings and other options, such as asynchronous connection options, are not available for RDP connections.
Setting Up ICA Connections

At least one ICA connection is required on a MetaFrame XP server for ICA Clients to use for establishing ICA sessions. After an ICA connection is set up, it exists even if no users are linked to the server with active ICA sessions. In contrast, an ICA session ordinarily exists on a MetaFrame XP server only while a user is linked to the server and using resources. When a user logs off from the MetaFrame XP server, the ICA session ends. However, if a connection breaks, an ICA session using the connection can remain active until its state is changed by Auto Client Reconnect or ICA Keep-Alive settings, or by a MetaFrame XP administrator using the Management Console for MetaFrame XP.

Multiple ICA Clients can establish ICA sessions through the same ICA connection on a MetaFrame XP server. MetaFrame XP associates a user ID and ICA connection with each ICA session.

You can set up one ICA connection on a MetaFrame XP server for each network transport protocol and adapter that ICA Clients use to link to the server.

MetaFrame XP supports the following ICA connection configurations:

**Network transport.** On Windows 2000 servers, TCP/IP, IPX, SPX, NetBIOS, and asynchronous (modem or direct cable connection). Terminal Services in Windows Server 2003 does not support remote connections over IPX/SPX, NetBIOS, and asynchronous transports.

**Network adapter.** Network interface cards (NIC), serial ports, and modems.

If your network uses TCP/IP and your MetaFrame XP server contains a NIC, users can launch sessions using an ICA connection configured for TCP and the NIC. To give dial-up access to remote users, you can also set up an ICA connection configured for a modem connected to a serial communication port on the MetaFrame XP server.

Using Citrix Connection Configuration

Citrix Connection Configuration is an enhanced version of the Windows utility Terminal Server Configuration (Windows 2000 Servers).

The Citrix Connection Configuration utility adds support for more connections and advanced configurations.
Use Citrix Connection Configuration to:

- Add network, asynchronous, and other types of connections
- Configure existing connections
- Set parameters for mapping client devices
- Set modem parameters
- Test modem configuration

To start Citrix Connection Configuration

From the Start menu, choose Programs > Citrix > MetaFrame XP > Citrix Connection Configuration.

From the Citrix Connection Configuration window, you can view the existing ICA connections. You can use the Connections menu to add, edit, or delete ICA connections.

For more information about procedures for adding and modifying connections, choose Contents from the Help menu in Citrix Connection Configuration.

Adding ICA Connections

If you install additional network protocols or modems, you can create ICA connections for users to access the MetaFrame XP server.

To add a network ICA connection

Use the following procedure to add an ICA connection for a network adapter. You might need to do this if, for example, you install an additional protocol such as IPX.

1. Run Citrix Connection Configuration (see “To start Citrix Connection Configuration”).
2. From the Connection menu, choose New. The New Connection dialog box appears:
3. Type a name for the connection in the **Name** box. You can enter an optional description in the **Comment** box.

4. From the **Type** list, select **Citrix ICA 3.0**.

5. From the **Transport** list, select the transport protocol.

6. Click **OK** to add the ICA connection. If a connection with these settings exists, a message tells you that a connection cannot be created with the same settings.

**Adding Asynchronous ICA Connections**

You can set up asynchronous ICA connections for access to MetaFrame XP servers. Asynchronous ICA connections can be dial-up connections through modems and direct cable (null modem) connections between the serial ports of a client device and MetaFrame XP server.

When you set up an asynchronous ICA connection in Citrix Connection Configuration, you avoid the overhead of Dial-Up Networking and TCP/IP on the server. MetaFrame XP supports modem configuration through the Windows Telephony Application Programming Interface (TAPI).

For the best performance over asynchronous connections, Citrix recommends using high-speed serial port hardware and processor-controlled multi-port adapters. Using hardware devices that place less demand on CPU resources allows more processor power to be devoted to running user sessions.
Important On a MetaFrame XP server, a modem or serial port cannot be configured as both a Dial-Up Networking port and an ICA asynchronous connection port. Also, you cannot configure an asynchronous direct cable connection using the Serial Cable between 2 PCs option in Windows Dial-Up Networking. Instead, you must configure the ICA asynchronous connection in Citrix Connection Configuration.

To add an asynchronous ICA connection

1. Run the Citrix Connection Configuration utility (see “To start Citrix Connection Configuration” on page 197).
2. From the Connection menu, choose New. The New Connection dialog box appears.
3. Type a name for the new connection.
4. From the Type list, select Citrix ICA 3.0.
5. From the Transport list, select async. Options for asynchronous connections appear in the dialog box.
6. From the Device list, select the COM port for the connection. Standard COM ports appear in the list. If a TAPI modem is installed on a COM port, the modem type follows the COM port name in the list. If a modem is installed on a particular COM port, you cannot select that COM port for a direct cable (null modem).
   - To install a modem, click Install Modem. Then, follow the instructions in the Install New Modem wizard to install and configure the modem.
   - To configure an existing modem, click Modem Properties.
7. Click OK to add the connection. If a connection with these settings exists, a message tells you that a connection cannot be created with the same settings.
Configuring Session Settings for ICA Clients

Three types of settings control the behavior of an ICA session:

**Per-connection settings.** You can use Citrix Connection Configuration to configure settings for each ICA connection. These settings are referred to as *per-connection settings* because they affect all ICA sessions that users establish through the ICA connection.

You can click Advanced, ICA Settings, and Client Settings in the New Connection or Edit Connection dialog box to configure per-connection settings.

For example, for a particular ICA connection, you can set a time-out value in the Advanced Connection Settings dialog box. This time-out setting will affect the sessions of all users who link to the server through that ICA connection.

Procedures for configuring per-connection settings appear later in this chapter.

**Per-user settings.** User and group settings that you configure in Windows will apply to any ICA connection. These settings, which are based on individual user accounts, include user names and group memberships, permissions, and dial-in settings.

For more information about per-user settings, refer to your Windows documentation. See the Windows online help for Local Users and Groups, or Active Directory Users and Computers.
**Per-client settings.** You can configure an ICA Client to enable additional security and compression. These settings apply to any ICA session established by that ICA client, independent of the person using the client device or the ICA connection used for the session.

For information about configuring per-client settings, see the *Citrix ICA Client Administrator's Guide* for each client that you deploy.

**Precedence of Settings**

A setting that you specify in Citrix Connection Configuration takes precedence over per-user and per-client settings. However, for some ICA connection settings, you can select an option to apply settings from user accounts or ICA Clients to the ICA connection.

- You can specify that an ICA connection use some settings from user accounts by selecting **Inherit User Config**.
- You can specify that an ICA connection use some settings from ICA Clients by selecting **Inherit Client Config**.

If you select one of these check boxes, the associated ICA connection settings are dimmed and cannot be edited. The setting specified by the Windows user account or ICA Client takes precedence over the ICA connection setting.

If you clear the check box for these options, the original ICA connection settings take effect.

---

**Important** You can create user policies to enable some connection settings for specific users or user groups. User policies override similar connection settings configured in Citrix Connection Configuration. However, if you disable functionality in Citrix Connection Configuration, you cannot enable the functionality by creating user policies. For more information about user policies, see “Creating and Applying User Policies” on page 281.
Configuring ICA Connection Options

This section discusses ways to configure options for ICA connections associated with network interfaces, modems, and direct cable (null modem) connections.

You can configure new ICA connections in the New Connection dialog box as described earlier in this chapter. To modify the configuration of an existing ICA connection, double-click the connection in the Citrix Connection Configuration window.

For more information about configuration procedures, see the online help in Citrix Connection Configuration.

**Configuring Modem Callback**

You can configure a modem ICA connection for modem callback. You can use this feature so that the call charges are incurred at the server end of the connection, or to provide a small measure of security.

To set modem callback options, use Citrix Connection Configuration.

When modem callback is active and a user dials in to the ICA connection on the MetaFrame XP server, the server modem answers, then hangs up, and dials a specified telephone number (the callback number) to reach the ICA Client modem and complete the connection.

Modem callback to a fixed number can provide a small level of security based on telephone numbers. Using this feature verifies that authorized users are dialing in by calling back to specified numbers to complete dial-in ICA connections.

To configure modem callback for a new ICA connection, use the options in the New Connection dialog box when you create a modem ICA connection.

To change the settings for an existing ICA modem connection, double-click the ICA connection in Citrix Connection Configuration. Then, use the Edit Connection dialog box to configure modem callback.
Enabling Modem Callback

You can enable or disable modem callback by using the first drop-down list and the adjacent check box in the Modem Callback area.

- Select the Inherit User Config check box to enable modem callback only for users who have modem callback enabled in their Windows user accounts. When this option is selected, the drop-down list is not available.

- From the drop-down list, choose To a fixed phone number or To a roving phone number to enable modem callback for all users.

- Choose Disabled from the drop-down list to disable modem callback for all users.

When you enable modem callback, you can specify one callback phone number for all users. You might do this if all users dial in from one phone number at a branch office, or you can use callback numbers from each user’s Windows account. Another option is to let users enter callback numbers when they make connections.

In Windows NT 4.0, you enter a callback phone number in the Dialin Information dialog box, which is available from the User Properties dialog box for each user account. In Windows 2000, you enter a phone number in the Dial-in tab of the Properties dialog box for each user account.

Specifying a Callback Number

To enable callback to a specified phone number, select To a fixed phone number in the first list. Type the telephone number in the Phone Number box. The connection will call back the phone number in the Phone Number box to establish the connection for all users—unless the Inherit User Config option next to the Phone Number box is selected. When Inherit User Config is selected, the Phone Number box is not available.

You can select the Inherit User Config option to use the callback configuration from the user’s Windows account configuration. If the user’s account is set to a specified phone number, that number is used, or user accounts can allow callers to enter callback numbers each time they connect.

For example, if users’ home phone numbers are specified in their user account configurations, you can choose To a fixed phone number and select the Inherit User Config option to ensure that users can dial in only from verified locations.
Using a Roving Phone Number

To enable callback and allow all users to enter the callback number, select **To a roving phone number** in the first drop-down list in the Modem Callback area. This setting prompts users to enter a callback number when they start an ICA session by modem. If a phone number is entered in the **Phone Number** box, this is the default number for callback.

You might want to use callback to a roving number so that remote users who dial in from hotels and other locations do not have to be responsible for phone charges for lengthy connections.

You can select the **Inherit User Config** box next to the **Phone Number** box. When this is selected, the **Phone Number** box is not available. The modem uses the callback configuration from the user’s Windows account. If the user’s account is set to call back a specified phone number, that number is used for callback. If **Set by Caller** is selected in the user’s account, the user can specify a callback number when making a connection.

Configuring Direct Cable Connections

You can use Citrix Connection Configuration to configure ICA connections for direct cable connections between serial (COM) ports on client devices and a MetaFrame XP server.

You can configure new connections in the **New Connection** dialog box when you create an asynchronous ICA connection.

To edit a connection, double-click the asynchronous ICA connection in Citrix Connection Configuration. Use the **Edit Connection** dialog box to configure the ICA connection.

Options for asynchronous cable (null-modem) ICA connections appear in the Async Transport Configuration area in the **New Connection** and **Edit Connection** dialog boxes.

With these options you can configure the following device and transmission properties for the ICA connection:
**Device.** Specifies the serial port (COM port) to use for the connection. The available COM ports on the MetaFrame XP server appear in the drop-down list.

**Device Connect On.** Specifies the signal type (CTS, DSR, RI, DCD, or First Character) for the server to use to determine when a connection is established and ready for user logon. You can select *Always Connected* to bypass connection detection.

**Baud.** Sets the communication rate for the connection. You can select standard baud rates from the drop-down list.

**Set Defaults.** Resets the Device Connect On and Baud settings, and the settings in the **Advanced Async Configuration** dialog box, to default values.

**Advanced.** Opens the **Advanced Async Configuration** dialog box for configuring additional serial port settings. These settings are described in the next section.

### Using the Async Test Dialog Box

You can test an asynchronous direct cable connection by using the **Test** button in the **New Connection** dialog box and the **Edit Connection** dialog box when you configure an async ICA connection.

The **Test** button appears in the Async Transport Configuration area when the Transport setting is Async and the selected Device is a COM port that does not have a modem installed on it.

The **Test** button opens the **Async Test** dialog box for testing communication through the specified serial port. In the dialog box, you can monitor control signals and transmit data to and receive data from a client device connected to the serial port.
The dialog box displays the name of the serial port and baud rate. A row of indicator “lights” shows the status of the DTR, RTS, CTS, DSR, DCD, and RI signals.

You can type text in the scrolling area to send ASCII data to a device that is connected to the specified serial port. The text you type does not appear in the dialog box unless a connected device echoes text that it receives.

If you transmit text from a terminal emulation program (such as HyperTerminal in Windows) that is running on a connected client device, the text appears in the Async Test dialog box if the connection is configured correctly.

**Configuring Advanced Async Options**

When you create or edit an async cable ICA connection, the Advanced button in the Async Transport Configuration area opens the Advanced Async Configuration dialog box. You can use this dialog box to configure flow control and other data transmission settings.

**Flow Control.** Select Hardware or Software flow control, or select None to configure the async connection with no flow control.

**Hardware Flow Control.** If you select Hardware in the Flow Control area, the options in the Hardware Flow Control area are available to specify signals used for flow control. Hardware flow control is the default configuration.
From the first drop-down menu, select the hardware signal action that indicates the receive buffer is full. From the second menu, select the hardware signal action that indicates data transmission can proceed. The default settings are “Turn off RTS when receive buffer is full” and “Transmit data when CTS is on.”

**Software Flow Control.** If you select Software in the Flow Control area, the options in the Software Flow Control area are available to specify the start and stop characters for data transmission.

Select Decimal or Hex to define character values, and then type decimal or hex values in the text boxes to set the Xon and Xoff characters for software flow control.

**DTR State.** The DTR State options are available with any flow control option unless Turn Off DTR is selected for Hardware Flow Control.

Select On to specify that the Data Terminal Ready (DTR) signal is always on. Select Off to specify that the signal is always off.
**RTS State.** These options are available with any flow control option unless Turn Off RTS is selected for Hardware Flow Control.

Select On to specify that the Request To Send (RTS) signal is always on. Select Off to specify that the signal is always off.

**Parity.** Click an option to specify the parity type or click None to specify no parity setting.

**Stop.** Select 1 or 2 to specify the number of stop bits per character.

**Byte.** This setting for the configuration of transmitted data cannot be changed because ICA protocol requires 8 bits per byte.

### Configuring Advanced ICA Connection Options

The **Advanced Connection Settings** dialog box provides additional control over security and performance on ICA connections. To use the dialog box, click the **Advanced** button when you create or edit an ICA connection.

The Advanced Connection Settings options for Windows connections apply to Citrix ICA connections. For more information about advanced options, see the Citrix Connection Configuration online help.
Restricting Connections to Published Applications

For high-security environments, select the **Only run published applications** check box to restrict the connection to run only published applications defined by the administrator. This option is not available unless you select **Inherit Client/User Config** in the Initial Program area.

**Note** You cannot specify a published application as the initial program.

MetaFrame XP provides additional options for controlling connections from ICA Clients, limiting ICA sessions, and restricting application usage. For more information, see “Controlling User Logons” on page 265 and “Controlling User Connections” on page 266.

### Configuring ICA Encryption

In the Security area, you can configure encryption for the ICA connection. Select an option from the **Required Encryption** menu.

The default encryption level is Basic. You can select strong encryption that applies the RC5 encryption algorithm with 128-bit minimum session keys to log on only or to all data transmission.

### Using Shadowing to Monitor ICA Sessions

*Shadowing* an ICA session means viewing the session from another device. During shadowing, you can monitor the session activity as if you were watching the screen of the ICA Client that initiated the session. You can see the active program running in the session, with the user’s keyboard input and mouse actions.

This section discusses settings for ICA connections related to shadowing. For information about how to shadow sessions, see “Shadowing ICA Sessions” on page 284.

While you are shadowing a session, if the MetaFrame XP server and ICA connection allow it, you can use your keyboard and mouse to remotely control the user’s keyboard and mouse in the shadowed session.

The ability to shadow ICA sessions depends on shadowing being enabled, as described next.
Enabling Shadowing on a Server

If you want to shadow ICA sessions, shadowing must be enabled on the MetaFrame XP server first and then for the ICA connections on the server.

You can enable shadowing on the MetaFrame XP server during installation of MetaFrame XP. To do this, you must select the default option, which allows shadowing on all ICA connections on the MetaFrame XP server. After you install MetaFrame XP, you can use Citrix Connection Configuration to limit or prohibit shadowing for specific ICA connections on the MetaFrame XP server.

If you select the option that allows shadowing, and also select options to restrict some aspects of shadowing, you cannot remove the restrictions using Citrix Connection Configuration. However, you can add shadowing restrictions for specific ICA connections on the server using Citrix Connection Configuration.

Prohibiting Shadowing on a Server

During installation of MetaFrame XP, if you select the option that prohibits shadowing, shadowing is not enabled for any ICA connections on the MetaFrame XP server. Any limits you set for shadowing during MetaFrame XP installation cannot be removed later in Citrix Connection Configuration.

Configuring ICA Connections for Shadowing

When you configure an ICA connection, you can use the Advanced Connection Settings dialog box to configure shadowing for the ICA connection.

If you want individual user configurations to take precedence over the ICA connection settings for shadowing, select Inherit User Config next to the Shadowing menu in the Advanced Connection Settings dialog box. This makes the Shadowing menu unavailable. For more information about user configuration, see “Precedence of Settings” on page 201.

When the Inherit User Config option is not selected, you can use the Shadowing menu to configure shadowing for an ICA connection. The shadowing settings affect all ICA sessions that use the ICA connection.
The settings in the **Shadowing** menu are in the form of statements that include terms (described in the following table) for shadowing status and features.

<table>
<thead>
<tr>
<th>Term</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enabled</td>
<td>Shadowing is possible for sessions on the ICA connection.</td>
</tr>
<tr>
<td>Disabled</td>
<td>Sessions on the ICA connection cannot be shadowed.</td>
</tr>
<tr>
<td>Input</td>
<td>Refers to using the keyboard and mouse for remote control of the shadowed session.</td>
</tr>
<tr>
<td></td>
<td>“On” means that the input from the mouse and keyboard are accepted for remote control from the device shadowing the session. “Off” means that this input is not accepted.</td>
</tr>
<tr>
<td>Notify</td>
<td>Refers to a notification message that MetaFrame XP sends to an ICA Client user. The message asks the user to allow someone to shadow the session. Users can accept or deny shadowing requests.</td>
</tr>
<tr>
<td></td>
<td>“On” means the server notifies users of all attempts to shadow sessions. “Off” means the server does not notify users, so they cannot deny permission or prevent shadowing.</td>
</tr>
</tbody>
</table>

For example, one option in the **Shadowing** menu states: “is enabled, input off, notify on.” This setting does the following: allows shadowing, prohibits remote control with the keyboard and mouse during shadowing, and requires the notification (and permission) of ICA Client users before anyone can shadow their sessions.

**Note** If you disable input for remote control or user notification when you install MetaFrame XP, options for these features are not available in the **Shadowing** menu in Citrix Connection Configuration. However, the options still appear in Microsoft’s user properties dialog box, but choosing them does not override the settings you select during MetaFrame XP installation. In general, you can use individual client properties to disable shadowing features on a per-user basis, but not to enable shadowing features that you disable on a MetaFrame XP server.
Configuring ICA Audio Settings

When you create or edit an ICA connection, you can use the ICA Settings button to configure audio for ICA Clients that connect to the MetaFrame XP server through that ICA connection.

When you click the ICA Settings button, the ICA Settings dialog box appears. From the drop-down list in the Client Audio Quality area, you can specify the audio quality to use for the connection. High, Medium, and Low audio quality settings are available.

**High.** This setting is recommended for connections only where bandwidth is plentiful and sound quality is important. This setting allows clients to play a sound file at its native data rate. Sounds at the highest quality level require about 1.3Mbps of bandwidth to play clearly. Transmitting this amount of data can result in increased CPU utilization and network congestion.

**Medium.** This setting is recommended for most LAN-based connections. This setting causes any sounds sent to the client to be compressed to a maximum of 64Kbps. This compression results in a moderate decrease in the quality of the sound played on the client device. The host CPU utilization can decrease compared with the non-compressed version due to the reduction in the amount of data sent across the wire.

**Low.** This setting is recommended for low-bandwidth connections, including most modem connections. This setting causes any sounds sent to the client to be compressed to a maximum of 16Kbps. This compression results in a significant decrease in the quality of the sound. The CPU requirements and benefits of this setting are similar to those of the Moderate setting; however, the lower data rate allows reasonable performance for a low-bandwidth connection.

**Sample.** You can click the Sample button to play a brief audio sample at the selected quality setting.
Audio mapping for ICA Clients can cause excessive load on the MetaFrame XP server and network. High quality increases bandwidth requirements by sending more audio data to ICA Clients. High quality audio also increases server CPU utilization.

ICA Client users can also select an audio quality setting. If settings on the client and server are not the same, the lower quality setting is used for the session.

In the **Client Settings** dialog box, you can disable audio for an ICA connection.

---

**Note** Audio mapping requires that sound hardware and drivers be installed and configured correctly on the MetaFrame XP server. The **Sample** button in the **ICA Settings** dialog box is not available if audio hardware is not detected by Citrix Connection Configuration.

---

**Configuring Client Device Mapping**

Citrix ICA Clients support mapping devices on client computers so they are available to the user from within a remote control ICA session. You do not need a network or RAS connection to use ICA Client device mapping. Client device mapping provides:

- Access to local drives, printers, and serial ports
- Cut-and-paste data transfer between an ICA session and the local clipboard
- Audio (system sounds and .wav files) playback from the ICA session

During logon, the ICA Client informs the server of the available client drives, COM ports, and LPT ports. By default, client drives are mapped to server drive letters and server print queues are created for ICA Client printers so they appear to be directly connected to the MetaFrame XP server.

These mappings are available only for the current user during the current session. They are deleted when the user logs off and recreated the next time the user logs on.

The MetaFrame XP server lists all client disk and printer devices in the Microsoft window that displays objects in the Client Network.

During a session, users can use ICA Printer Configuration to map client devices not automatically mapped at logon. For more information about using the ICA Printer Configuration utility, see the *Citrix ICA Client Administrator’s Guides* for the clients you plan to deploy.
Options for Client Device Mapping

Client device mapping options are specified in the Client Settings dialog box in Citrix Connection Configuration.

The Connection options control whether or not drives and printers are mapped to client drives and printers. If these options are cleared, the devices are still available but must be mapped to drive letters and port names manually.

Connect client drives at logon. If this option is checked, the client computer’s drives are automatically mapped at logon.

Connect client printers at logon. If this option is selected, MetaFrame XP maps printers that are configured on client devices with ICA Clients for Windows. With ICA Clients for DOS, users can manually map printers.

Default to main client printer. If this option is checked, the user’s default client printer is configured as the default printer for the ICA session.

Inherit user config. If this option is selected, the per-user settings in User Manager are used.

To automatically connect to only the printer configured as the default printer when the user logs on, select the By default, connect only the client’s main printer check box.

Default printers can be set on the ICA Client device. Users can override the default printer mapping with ICA Client Printer Configuration. For more information about ICA Client Printer Configuration, see the Citrix ICA Client Administrator’s Guides for the clients you plan to deploy.

Click Client Mapping Overrides to disable client device connections.

Client Drive Mapping

Client drive mapping is built into the standard Citrix MetaFrame device redirection facilities. The client drives appear as client network objects in Windows. The client’s disk drives are displayed as shared folders with mapped drive letters. These drives can be used by Windows Explorer and other applications like any other network drive.
How MetaFrame XP Assigns Drive Letters to Mapped Client Drives

By default, the drives on the client system are automatically mapped to drive letters on the MetaFrame XP server when users log on. The server tries to match the client drives to the client drive letters; for example, the client’s first floppy disk drive to A, the second floppy disk drive to B, the first hard drive partition to C, and so forth. This allows the user access to client drive letters in the same way from local or remote sessions.

These drive letters are often used by the drives on the MetaFrame XP server. In this case, client drives are mapped to other drive letters. The MetaFrame XP server starts at V and searches in ascending order for free drive letters.

Reassigning Server Drives

For an ICA session, a MetaFrame XP server tries to map disk drives on a client device to the typical drive letters for the client. If the drive letters are available, the server maps the client’s first floppy disk drive to A, the second floppy drive to B, the first hard disk drive to C, and so on. However, a server cannot map client device drives to letters that are assigned to the server’s own disk drives.

Run DriveRemap.exe, located on the MetaFrame XP server CD, to change the drive letters of the MetaFrame XP server. For more information about the DriveRemap utility, see “DRIVEREMAP” on page 338. By changing the server to use drive letters that are higher, such as M, N, and O, the original lower drive letters become available for assignment to the drives on client devices. This can make the use of drives on client devices less confusing for users, because they see their drives identified by typical drive letters.

If you want to change server drive letters, Citrix recommends that you do so before installing MetaFrame and before installing applications on the MetaFrame XP server. Changing server drive letters after MetaFrame XP installation can cause unstable performance by the server, components of the operating system, and installed applications.

CAUTION   With utilities provided in Windows, it is possible to change server drive letters after MetaFrame XP installation. Citrix advises against changing server drive letters after MetaFrame XP installation. Doing so can destroy data stored on disk drives and can leave MetaFrame XP and the operating system unable to operate.
Controlling Drive Mapping When Using NetWare Logon Scripts

Client drive mapping and NetWare logon script execution occur in parallel. If the logon script maps NetWare network drives, it is possible that a user could find drive V mapped to his client drive C during one session but mapped to a NetWare drive during another.

You can avoid this problem by adding two registry values in HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\InitialNetwareDrive:

- **CAUTION** Using Registry Editor incorrectly can cause serious problems that can require you to reinstall the operating system. Citrix cannot guarantee that problems resulting from incorrect use of Registry Editor can be solved. Use Registry Editor at your own risk.

Make sure you back up the registry before you edit it. If you are running Windows NT, make sure you also update your Emergency Repair Disk.

**REG_SZ: InitialClientDrive**
Defines the first drive letter to use for client drive mapping. The system searches backward through the alphabet to assign drive letters to client drives that could not be mapped to their “native” drive letters.

**REG_SZ: InitialNetWareDrive**
Defines the drive letter to use for the NetWare SYS:LOGIN directory that is mapped to the preferred server during the initial NetWare attachment. This setting is the equivalent of the DOS VLM Net.cfg setting “First Network Drive.” If this value is not set, the first available drive letter starting with C and working up to Z is used for this mapping.

Client Printer Mapping

Client printer mapping allows a remote application running on a MetaFrame XP server to access client printers (printers that are attached locally to client devices). The client mappings appear as another network type, Client Network, to the Windows Print Manager.

MetaFrame XP maps client printers when a user logs on and deletes client printers when the user logs off, if the printers do not contain unfinished print jobs. If the print queue contains print jobs, you can set MetaFrame XP to retain the printer and the print jobs.
For more information about client printers and printer management in MetaFrame XP server farms, see “Managing Printers for ICA Clients” on page 291. For information about specific ICA Clients, see the *Citrix ICA Client Administrator’s Guide* for each ICA Client you use.

**Client Serial Port Mapping**

Client COM port mapping allows a remote application running on the MetaFrame XP server to access devices attached to COM ports on the client device. Client COM ports are not automatically mapped to server ports at logon, but can be mapped manually using the `net use` or `change client` commands. See Appendix A, “MetaFrame XP Command Reference,” for more information about the `change client` command.

For more information about client COM port mapping, see the *Citrix ICA Client Administrator’s Guides* for the clients you plan to deploy.

**Client Audio Mapping**

Client audio mapping allows applications running on the MetaFrame XP server to play sounds through a sound device on the client device. DOS and Win16 ICA Clients require Sound Blaster 16-compatible sound cards. ICA Win32 Clients require any Windows-compatible sound card; the ICA Win32 Client uses standard Windows API calls for audio.

The MetaFrame XP server can control the amount of bandwidth used by client audio mapping. Audio mapping is configured per-client and per-connection in the **ICA Settings** dialog box.

For more information about using client audio mapping, see the *Citrix ICA Client Administrator’s Guides* for the clients you plan to deploy.
Deploying ICA Clients to Users

This chapter addresses issues to help you plan and implement your deployment of ICA Client software to end users.

Choosing a Deployment Method

To access applications on MetaFrame XP servers, users run ICA Client software on their client devices. You can deliver the appropriate ICA Client to your users and install the software with the following methods:

- Using Microsoft Systems Management Server (SMS) or Active Directory Services in Windows (for ICA Clients that can be installed with Windows Installer packages)
- Using a Web browser
- Downloading from a network share point
- Using installation diskettes

Tip If you are updating the ICA Clients, use the Client Update Database to deploy the latest versions of the ICA Client software.

If you are a system administrator for a small company with users in one physical location, installing the ICA Client software from floppy disks or from a network file server presents few problems.

You can eliminate user involvement in the installation process by installing the ICA Client software on each user’s machine using a set of floppy disks or the MetaFrame XP Components CD. This method is useful if your users have limited computer experience.
If your users have a moderate level of computer expertise, you can direct them to a network share point containing the ICA Client files. You can send users an e-mail message that contains both a link to the installation files and instructions for installing the software. Installation by users can eliminate the need for you to manually install ICA Client software.

In a large enterprise or an application service provider (ASP) environment, with hundreds or thousands of users in multiple locations, manual installation methods are not efficient. In these situations, Web delivery of ICA Client software or deploying with Active Directory or Microsoft Systems Management Server are the best choices.

The table below lists common computing environments and the appropriate deployment methods to use in each scenario.

<table>
<thead>
<tr>
<th>Organization</th>
<th>Deployment method</th>
<th>Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enterprise, ASP supplying personalized content and published applications</td>
<td>Web Interface for MetaFrame XP</td>
<td>Users click links on their desktops or run a supported Web browser (see the Web Interface Administrator's Guide for a full list).</td>
</tr>
<tr>
<td>Enterprise, ASP, small business</td>
<td>Active Directory or Systems Management Server (SMS)</td>
<td>Users download ICA Client software from a centralized location. See your Windows or SMS documentation for more information.</td>
</tr>
<tr>
<td>Enterprise, ASP, small business</td>
<td>Web-based installation</td>
<td>Users run a Web browser to access an ICA Client download Web site and install software.</td>
</tr>
<tr>
<td>Enterprise, small business</td>
<td>Network share point</td>
<td>Users connect to a network share point and install software.</td>
</tr>
<tr>
<td>Small business (single site); organization with remote users who require ICA Client installation diskettes</td>
<td>Diskettes</td>
<td>Client devices have floppy disk drives.</td>
</tr>
</tbody>
</table>
Delivering Applications to Users

To choose the best method for deploying the ICA Clients, decide how your end users will access published applications.

If you want to deliver applications to your users by a Web page, use the Web Interface for MetaFrame XP in conjunction with MetaFrame XP Server, or the Application Launching and Embedding (ALE) feature in MetaFrame XP. When you deliver applications using a Web-based method, users click links on their desktops using the Program Neighborhood Agent or launch Web browsers to access applications published on MetaFrame XP servers.

If you do not want to deliver applications to your users through a Web page, publish the applications for direct access. To directly access applications published on MetaFrame XP servers, users launch ICA Client software. Using the ICA Win32 Client, users can launch Program Neighborhood to access the applications they are authorized to use on the MetaFrame XP servers. Using the ICA Win16 Client, users launch Remote Application Manager to establish connections to servers and published applications.

Providing Application Access with the Web Interface for MetaFrame XP

If you implemented or plan to implement a corporate Web-based portal, use the Web Interface for MetaFrame XP to integrate personalized application sets and information into your company’s Web site. With the Web Interface, users can access published applications through program icons on their desktops, in their Start menus (with the Program Neighborhood Agent), or through Web browsers.

A Web-integrated MetaFrame XP system consists of three components: a MetaFrame XP server farm, a Web server, and client devices. When a user logs on to the Web Interface for MetaFrame XP, the Web-based ICA Client Installation feature checks the user’s computer for the presence of ICA Client software. If the ICA Client software is not detected, the Web-based ICA Client Installation feature presents the appropriate ICA Client software for download and setup.
Important  You can install the Web Interface on the MetaFrame XP server as part of MetaFrame XP Setup. Install the Web Interface on the MetaFrame XP server only if IIS 4.0 or IIS 5.0 is also present on the server.

If you choose to install the Web Interface, a Web site is installed on your MetaFrame XP server in a Citrix directory under the Web document root; for example, c:\inetpub\wwwroot\citrix\NFuse.

This Web site contains logic that at runtime references the server’s document root directory for the presence of ICA Clients. To use the ICA Client installation feature of the Web Interface, copy the ICA Clients from the Icaweb directory on the MetaFrame XP Components CD to a directory named Icaweb in the Citrix directory in the Web document directory; for example, c:\inetpub\wwwroot\citrix\icaweb.

You must copy the entire Icaweb directory to this directory to enable Web-based ICA Client installation from the Web Interface.

If you plan to use the Web Interface for MetaFrame XP, see the Web Interface Administrator’s Guide for more information. If you do not plan to use the Web Interface, but want to deploy ICA Client software using the Web, see “Web-Based Installation” on page 226.

Application Launching and Embedding

If you are not planning to use the Web Interface for MetaFrame XP but want to deliver published applications to your users on a Web page, you can use Application Launching and Embedding (ALE). ALE allows users to run applications published on MetaFrame XP servers by clicking hyperlinks on a Web page.

For more information about Application Launching and Embedding, see “Creating Files for Application Launching and Embedding” on page 254. For more information about using the Citrix ICA Win32 Client with Application Launching and Embedding, see the Administrator’s Guide for the ICA Win32 Client.

Determining the Scope of ICA Client Deployment

Take the following factors into consideration before you decide which deployment method to adopt:

The ICA Clients you need to deploy.  To determine which ICA Clients you need to deploy, determine which client devices and operating systems you need to support.
A smaller organization with many similar client devices might need to deploy the ICA Client on only one or two platforms. In this scenario, using installation diskettes or copying the necessary files to a central network share point for download are the most efficient deployment methods.

Heterogeneous computing environments and geographic separation of large enterprises and ASPs can make it impossible to predetermine which client devices need to be supported. In these scenarios, Web-based installation is the most efficient deployment method.

**Centralized control and configuration requirements.** Determine what limits you need to impose on users’ access to published applications. You can configure various settings before you initially deploy the ICA Clients.

For information about preconfiguring ICA Clients, see the *Administrator’s Guide* for the required ICA Client or the Support area of the Citrix Web site at http://www.citrix.com.

**Ease-of-use requirements for users.** Providing a simple installation process that requires little interaction from users might be a key factor.

Enterprises and ASPs with hundreds or thousands of users with varied computing expertise require the most foolproof deployment process. You can “push” the ICA Client software to your users by various methods, including through the use of logon scripts or windows scripts, or through the use of a commercial software distribution package.

## Using the MetaFrame XP Components CD

The MetaFrame XP Components CD contains setup and installation files for all ICA Clients. You can use the MetaFrame XP Components CD to directly install ICA Client software on client devices that have CD-ROM drives, or copy the CD image to a network share point on a file server. For more information about installing ICA Client software, see the *Administrator’s Guide* for the required ICA Client.

You can copy the necessary files from the MetaFrame XP Components CD to your server using the ICA Client Distribution wizard. You can then access the ICA Client files from your server.

The ICA Client Distribution wizard appears during MetaFrame XP Setup. If you skipped this step during MetaFrame XP Setup, you can run the wizard by choosing **Start > Programs > Citrix > MetaFrame XP > ICA Client Distribution Wizard**.

Use the ICA Client Distribution wizard to:

- Create or update ICA Client images on your server
Create or update the ICA Client Update Database

Install the Administrator’s Guides for all ICA Clients

For detailed instructions about running the ICA Client Distribution wizard, see “Installing ICA Client Software” on page 127.

Pass-Through ICA Client

When you run MetaFrame XP Setup, you can install the pass-through ICA Win32 Client on the server. You can install the full ICA Win32 Program Neighborhood Client or the Program Neighborhood Agent.

Install the pass-through ICA Win32 Program Neighborhood Client if you want to give users who run other ICA Clients access to the features of Program Neighborhood. Users launch Program Neighborhood from the server desktop or as a published application. When users connect to the Program Neighborhood published application, they can launch all other applications published on the MetaFrame XP servers in your farm from a single interface.

Install the pass-through ICA Win32 Program Neighborhood Agent if you want to give users who run other ICA Clients transparent access to published applications from the server desktop. When you use the pass-through Program Neighborhood Agent, links to published applications appear in the Start menu and the Windows System Tray and shortcuts appear on the server’s desktop. Users can launch published applications from the server desktop; they do not have to open the Program Neighborhood application.

ICA Client Object

The ICA Client Object specification makes available a set of application programming interfaces (APIs) to the ICA Win32 Client. Any application that supports object embedding can interface with and pass instructions to this ICA Client.

The APIs give MetaFrame XP administrators, Web developers, and advanced users of the ICA Client software the ability to programmatically control the appearance and behavior of the ICA Win32 Client. With these APIs you can:

- Use the ICA Client Object with commercial desktop applications that support object embedding, including standard Web browsers such as Internet Explorer and Netscape, as well as the Microsoft Office suite of business applications.
- Integrate ICA functionality into third-party applications.
- Use the ICA Client Object APIs within custom scripts (Visual Basic and HTML) to programmatically integrate and manipulate the appearance and behavior of the ICA Client.
Chapter 9 Deploying ICA Clients to Users 225

For more information about the ICA Client Object, see the Citrix ICA Client Object Programmer’s Guide, located on the MetaFrame XP Components CD.

Deploying the ICA Clients

The following section explains how to deploy the ICA Clients using Web-based installation, from a network share point, and with installation diskettes.

You can integrate components of the methods that follow with your existing electronic software distribution system, or create scripts that permit an unattended install of the ICA Client software on your users’ devices.

Using Installer Packages for Client Deployment

The ICA Client for Win32—full Program Neighborhood and Program Neighborhood Agent versions—are both available in Microsoft Windows installer packages (.msi files), so you can use Windows Installer technology to deploy and install them. You can distribute the ICA Win32 Client installer package files to users by using Microsoft Systems Management Server (SMS) or Active Directory Services in Windows.

See your Windows or Systems Management Server documentation for more information.

The ICA Win32 installer package files are located in the following directories (substitute language with the language of the ICA Client software) on the MetaFrame XP Components CD included in the MetaFrame XP media pack:

icaweb\language\ica32

where language is one of:

• En (English)
• Fr (French)
• De (German)
• Ja (Japanese)
• Es (Spanish)

The installer package for the Program Neighborhood Agent is also located in the directory icainst\language\ica32\pnagent.

Note The Windows Installer service is present by default on computers running Windows 2000 or Windows XP. If the computer is running Windows NT 4.0 or Windows 9x, you must install Windows Installer.
Web-Based Installation

More companies are turning to Web-based technology to deliver information and applications to their employees. For large enterprises and ASPs, Web-based delivery can greatly automate repetitive tasks and centralize control of configuration options. Large organizations naturally want to minimize user involvement with software installation.

For companies that are not using the Web Interface for MetaFrame XP, Citrix offers an installation method that uses a Web browser on the client device as the interface for downloading the ICA Client. Users access a setup page containing a link to the appropriate ICA Client setup program.

If you want to set up an ICA Client download Web site on a Windows-based Web server, you can download the components and documentation for Web-based installation from the download area of the Citrix Web site at http://www.citrix.com/download.

**Tip** If you are planning to use the Web Interface for MetaFrame XP, see the Web Interface Administrator’s Guide for information and instructions about deploying the ICA Clients using the Web Interface.

Deploying ICA Clients over a Network

- **To deploy ICA Client software from a network share point**
  1. If you have not done so already, run the ICA Client Distribution wizard to copy the ICA Client files from the MetaFrame XP Components CD to your MetaFrame XP server.
  2. Copy the ICA Client files to a network share point. For example, if you are deploying the ICA Win32 Client, copy all files from \ICA32. The ICA Client Distribution wizard copies this folder to the location (installdir)\System32\clients\Ica on the server.
  3. Supply your users with the path to the client software setup program.
  4. To install the ICA Client software, launch Setup to begin the installation process. For more information about installing the ICA Clients from a network share point, see the Administrator’s Guide for the required ICA Client.
Deploying ICA Clients Using Diskettes

Use the ICA Client Creator to create installation disks for the ICA Client for DOS, the ICA Client for Windows 95/98/Me/NT/XP, and the ICA Client for Windows 3.x. The procedure is described below. For more information about installing the ICA Clients from installation diskettes, see the Administrator's Guide for the required ICA Client.

Note The ICA Client Creator utility is not supported on MetaFrame XP servers running on the Windows Server 2003 operating system.

Installation files for other ICA Clients are contained in the following folder: \installdir\System32\clients\Ica. You can copy the files for the required ICA Client to create installation diskettes.

You can also distribute diskettes to remote users who require the ICA Client but do not have access to a common network share point.

To use the ICA Client Creator to make installation diskettes

1. If you have not done so already, run the ICA Client Distribution wizard to copy the ICA Client files from the MetaFrame XP Components CD to your MetaFrame XP server.
2. From the Start menu, choose Programs > Citrix > MetaFrame XP > ICA Client Creator. The Make Installation Disk Set dialog box appears.
3. Select the desired ICA Client. The dialog box displays the number of disks you will need.
4. Select Format Disks to format the disks when creating the installation media.
5. Click OK and follow the directions to copy the ICA Client files to diskettes.

Updating the ICA Clients

Use the Client Auto Update feature to update ICA Client installations with new versions of ICA Client software. As new versions of ICA Clients are released by Citrix, you add them to the Client Update Database. New versions of ICA Clients are released periodically and can be downloaded from the Citrix Web site at http://www.citrix.com/download.
When users log on to a MetaFrame XP server, the server queries the ICA Client to determine the version number. If the version matches the one in the Client Update Database, the logon continues. If the server detects an older version on the client device, the user is informed that a newer version of the ICA Client is available for download. The user can update the client according to the options you set in the database.

Client Auto Update works with all transport types supported by ICA (TCP/IP, IPX, NetBIOS, and asynchronous). Client Auto Update supports the following features:

- Automatically detects older ICA Client files
- Copies new files over any ICA connection without user intervention
- Provides administrative control of update options for each ICA Client
- Updates ICA Clients from a single database on a network share point
- Safely restores older ICA Client versions when needed

**Important** Client Auto Update can update client files to newer versions of the same product and model. For example, it can update the ICA Win32 Client to a new version. It cannot upgrade the ICA Win16 Client to the ICA Win32 Client. In addition, you cannot automatically update previous versions of the ICA Win32 Client installed with Windows Installer packages (.Msi type files). You must redeploy an ICA Win32 Client Windows Installer package when a new version of this client is released.

**The ICA Client Update Process**

ICA Clients are identified by platform with a product and model number. The version number is assigned when new ICA Clients are released.

The process of updating ICA Clients with new versions uses the standard ICA protocol.

- If an update is needed, by default, the MetaFrame XP server informs the user that a new client is available and asks to perform the update. You can specify that the update occurs without informing the user and without allowing the user to cancel the update.

- By default, the user can choose to wait for the client files to finish downloading or to download the files in the background and continue working. Users connecting to the MetaFrame XP server with a modem get better performance waiting for the update process to complete. You can force the client update to complete before allowing the user to continue.
During the update, new ICA Client files are copied to the user’s computer. You can force the user to disconnect and complete the update before continuing the session. The user must log on to the MetaFrame XP server again to continue working.

When the user disconnects from the server and closes all client programs, the ICA Client update process finishes.

As a safeguard, the existing ICA Client files are saved to a folder named Backup in the Citrix\ICA Client subdirectory of the Program Files directory on the user’s local drive.

Configuring the Client Update Database

You can configure a Client Update Database on each MetaFrame XP server in a server farm, or configure one database to update the ICA Clients for multiple MetaFrame XP servers.

Use the ICA Client Distribution wizard to create or update the ICA Client Update Database. The wizard appears during MetaFrame XP Setup. If you skipped the wizard during MetaFrame XP Setup, run the wizard by selecting Start > Programs > Citrix > MetaFrame XP > ICA Client Distribution Wizard. For more information about the ICA Client Distribution wizard, see page 127.

The Client Update Database contains the following ICA Clients: 32-bit Windows, 16-bit Windows, 32-bit DOS, Macintosh, and several WinCE Clients. As new versions of the ICA Clients are released by Citrix, you add them to the Client Update Database.

Using the Client Update Configuration Utility

Use the Client Update Configuration utility to manage the client update database. From this utility, you can:

- Create a new update database
- Specify a default update database
- Configure the properties of the database
- Configure client update options
- Add new ICA Clients to the database
- Remove outdated or unnecessary ICA Clients
- Change the properties of an ICA Client in the database

The following sections give an overview of the Client Update Configuration utility. For details, see the utility’s online help.
To access the ICA Client Update Configuration utility
1. From the Start menu, choose Programs > Citrix > MetaFrame XP > ICA Client Update Configuration.
2. The ICA Client Update Configuration window appears. The status bar shows the location of the current update database, which the MetaFrame XP server uses to update ICA Clients. The window shows the ICA Clients in the database.

Creating a New Client Update Database
The ICA Client Distribution wizard creates the Client Update Database in the location %Program Files%\Citrix\ICA\ClientDB. You can create a new update database in any location on a server disk or on a network share point.

To create a new update database
1. From the Database menu, choose New. The Path for the new Client Update Database dialog box appears.
2. Enter the path for the new update database and click Save. The utility creates a new update database in the specified location and opens the new database.

Specifying a Default Client Update Database
You can configure one Client Update Database to be used by multiple MetaFrame XP servers. If the Client Update Database is on a shared network drive, use the ICA Client Update Configuration utility to configure your MetaFrame XP servers to use the same shared database.

To set the default database for MetaFrame XP servers
1. From the Database menu, choose Open.
2. Specify the path to the default database and click Open. The database opens.
3. On the Database menu, click Set Default. The Set Default Database dialog box opens:
4. Select **Set as Default Database on Local Machine** to make the currently opened database the default database. You can also set other MetaFrame XP servers to use the currently open database as the default database.

5. Double-click a domain name to view the servers in that domain. Click a server to set its default database to the currently open database. You can select multiple servers by holding down the CTRL key and clicking each server.

6. Click **OK**.

**Configuring Default Client Update Options**

Use the **Database Properties** dialog box to configure overall database-wide settings for the current Client Update Database. Choose **Properties** from the **Database** menu to display the dialog box.
The **Database Path** box displays the path and file name of the database you are configuring.

The **Enabled** check box must be selected for this database to perform ICA Client updates.

**Tip** If the ICA Clients do not need to be updated, disable the database to shorten your users’ logon time.

The options in the **Default update properties for clients** section specify the default behavior for the ICA Clients added to the database. You can also set properties for individual ICA Clients (as described later in this chapter). Individual ICA Client properties override the database properties.

- Under **Client Download Mode**, select **Ask user** to give the user the choice to accept or postpone the update process. Select **Notify user** to notify the user of the update and require the client update. Select **Transparent** to update the user’s ICA Client software without notifying or asking the user.

- Under **Version Checking**, select **Update older client versions only** to update only client versions that are older than the new client. Select **Update any client version with this client** to update all client versions to this version; choose this option to force an older client to replace a newer client.
Chapter 9  Deploying ICA Clients to Users

- Under **Logging**, select **Log downloaded clients** to write an event to the event log when a client is updated. By default, errors that occur during a client update are written to the event log. Clear the **Log errors during download** check box to turn this option off.

- Under **Update Mode**, select the **Force disconnection** option to require users to disconnect and complete the update process after downloading the new client. The **Allow background download** option is selected by default to allow users to download new client files in the background and continue working. Clear this check box to force users to wait for all client files to download before continuing.

- Specify the number of simultaneous updates on the server. When the specified number of updates is reached, new client connections are not updated. When the number of client updates is below the specified number, new client connections are updated.

Click **OK** when you finish configuring the database settings.

### Adding ICA Clients to the Client Update Database

When you want to deploy a newer version of the ICA Client, add it to the Client Update Database. You can download the latest ICA Clients from the Citrix Web site at http://www.citrix.com/download.

- **To add a Citrix ICA Client to the Client Update Database**
  1. From the **Client** menu, click **New** to display the **Description** screen.
  2. In the **Client Installation File** box, browse to or enter the path to the client installation file Update.ini. If you ran the ICA Client Distribution wizard, you can find the Update.ini file in the location `%Program Files%\Citrix\ICA\ClientDB`. You can also find the Update.ini file on the MetaFrame XP Components CD.
  3. The client name, product number, model number, and version number are displayed. The **Comment** text box displays a description of the new client. You can modify this comment. Click **Next** to continue.
  4. The **Update Options** dialog box appears. The options in this dialog box specify how the client update process occurs for this client. The database-wide update options are displayed. You can specify different behavior for individual clients.
For definitions of the options in this dialog box, see “Configuring Default Client Update Options” on page 231 or see the online help for this dialog box. Click **Next** when you finish configuring the client update options.

5. The **Event Logging** dialog box appears.

The database-wide logging options are displayed. You can specify different behavior for individual clients. Select **Log Downloaded Clients** to write an event to the event log when this client is updated. By default, errors that occur during a client update are written to the event log. Clear the **Log Errors During Download** check box to turn this option off. Click **Next** to continue.

6. The **Enable Client** dialog box appears.

The Client Update Database can contain multiple versions of an ICA Client with the same product and model numbers. For example, when Citrix releases a new version of the ICA Win16 Client, you add it to the Client Update Database. However, only one version of the client can be enabled. The enabled client is used for client updating.

7. Click **Finish** to copy the ICA Client installation files into the Client Update Database.
Removing an ICA Client from the Client Update Database

It is important to delete ICA Clients that are not used from the Client Update Database. A database that contains multiple versions of the same client significantly slows the checking procedure that is carried out each time a user connects to the server.

- To remove an ICA Client from the database
  1. Select the ICA Client you want to remove from the database.
  2. From the Client menu, choose Delete. A message asks you to confirm the deletion.
  3. Click Yes to remove the client.

Changing the Properties of an ICA Client in the Database

Use the Properties dialog box to set properties for an individual ICA Client. Individual ICA Client properties override the database properties.

- To change the properties of an ICA Client in the Client Update Database
  1. Select the client you want to change.
3. The **Description** tab lists the client name, product number, model number, and version number. Select the **Enabled** check box to update the same platform ICA Client to this version. Optionally, enter a new comment in the **Comment** box.

4. Use the **Update Options** tab to configure update options for the client.
   - Under **Client Download Mode**, select **Ask user** to give the user the choice to accept or postpone the update process. Select **Notify user** to notify the user of the update and require the client update. Select **Transparent** to update the user’s ICA Client software without notifying or asking the user.
   - Under **Version Checking**, select **Update older client versions only** to update only client versions that are older than the new client. Select **Update any client version with this client** to update both earlier and later versions of the client to this version. Select this option to force an older client to replace a newer client.
   - Select the **Force Disconnection** option to require users to disconnect and complete the update process after downloading the new client.
   - Select the **Allow Background Download** option to allow users to download new client files in the background and continue working. Clear this check box to force users to wait for all client files to download before continuing.
   - Type a message to be displayed to users when they connect to the server.

5. Use the **Event Logging** tab to configure logging settings for this client.
   - Select the **Log Downloaded Clients** option to write an event to the event log when a client is updated.
   - Select the **Log Errors During Download** option to write errors that occur during a client update to the event log.

6. Use the **Client Files** tab to view the list of files associated with this client.
   - The Client Update Database stores the following information about each client file: file name, group, flags, file size, and file CRC.

7. Click **OK** when you finish configuring the settings for the client.

**ICA Client Deployment Practices**

This section provides examples of ICA Client deployment practices for a large manufacturing enterprise, a regional bank, an application service provider, and an insurance company.
**Manufacturing Enterprise**

The Best Paper Company employs approximately 30,000 people, located in shop-floor sites and remote offices in several countries. The enterprise has many pockets of MetaFrame XP installations, each owned and managed by a different team. Published applications include PeopleSoft and Oracle Manufacturing and Financials.

The networking environment includes the following:

- Ethernet LANs
- Frame Relay WAN
- Internet connections for remote users
- TCP/IP network protocol
- Thousands of 486 PCs running Windows 95
- Thousands of Pentium PCs running Windows 2000

The Best Paper Company is using the Web Interface for MetaFrame XP to give users access to critical applications. The company’s existing MetaFrame XP server farms function as an application serving back-end. The server farm supplies application set information and hosts published applications.

Application sets are delivered to groups or individual users, based on their role in the company. An employee launches a Web browser to access the Web Interface logon page. When the employee is authenticated to the server farm, the application set assigned to the employee is displayed within the browser. To start an application, the employee clicks a hyperlink on the Web Interface logon page.

The company uses the Web Interface’s built-in Web-based ICA Client Installation feature to deploy the ICA Client software. When a user launches an application, the user’s computer is checked for the ICA Client software. If the client is not detected, the user’s platform is identified and the appropriate ICA Client software is presented for download and setup.

The Web browser and ICA Client work together as viewer and engine. The browser displays the user’s application sets and the ICA Client launches applications.

For more information about the Web Interface for MetaFrame XP, see the *Web Interface Administrator's Guide*.

**Regional Bank**

Lenders Bank has 500 employees in its headquarters and 15 branch locations. The bank’s staff connects to MetaFrame XP servers to run more than 60 applications, including Ceridian and Transcend-Banker financial applications, Microsoft Office 2000, Microsoft Outlook, and AS/400 applications.
The networking environment includes the following:

- Ethernet LANs
- Secured Fractional T1, 56K leased lines
- TCP/IP network protocol
- One hundred 486 PCs, Wyse Winterm Windows-based terminals

The bank’s IT department used the Web-based ICA Client Installation package (without using the Web Interface for MetaFrame XP) to construct an ICA Client download Web site, integrated into the bank’s Intranet, for ICA Client software deployment. The IT department posted user-friendly instructions that walk users through downloading and installing the ICA Client software.

For more information about constructing an ICA Client download Web site, see “Using Installer Packages for Client Deployment” on page 225 of this guide. The elements required to construct an ICA Client download Web site can also be obtained from the Citrix Web site at http://www.citrix.com/download.

**Application Service Provider**

LinkToUs, a commercial ASP, has four data centers, located in the United States, Canada, and Ireland, serving over 100,000 end-users worldwide. LinkToUs offers its customers the following connection options:

- Internet
- Virtual Private Network (VPN)
- Frame Relay
- X.25 connections in more than 105 countries
- Private point-to-point lines

LinkToUs customers can choose from a variety of published application set packages, which can include applications from Microsoft, Onyx, Great Plains, Sales Logic, and Pivotal.

With the implementation of the Web Interface for MetaFrame XP, LinkToUs is now also designing and hosting highly customized corporate entry portals providing application integration, personalized Web content, external Web content integration, and search and categorization features.

LinkToUs works closely with its customers to develop user groups that meet their needs, and then builds application sets based on these groups. The ASP can display published applications from several MetaFrame server farms, including MetaFrame XP for Windows and MetaFrame for UNIX servers, in a single Web page.
The Web developers at LinkToUs created a simple script that allows automatic download and installation of the ICA Win32 Web Client. When end-users access the corporate portal hosted by LinkToUs for the first time, the ICA Client is automatically downloaded and installed on the user’s computer.

For more information about the Web Interface for MetaFrame XP, see the *Web Interface Administrator’s Guide*. For more information about automatic download and installation of the ICA Clients for the Web, see the Online Knowledge Base, accessible from the Support area of the Citrix Web site at http://www.citrix.com.

**Insurance Company**

Protection Insurance is a mid-sized company with 800 employees. Published applications include PeopleSoft and customized applications for the insurance industry from JDE and Prelude. The networking environment includes:

- Ethernet LAN, Internet, and dial-up connections
- TCP/IP network protocol
- Pentium PCs running Microsoft Windows NT

The purchasing department preconfigures users’ systems to include the latest version of the ICA Win32 Client. When applications are published, a shortcut to each application is placed on the user’s Start menu. Users can also launch Program Neighborhood to access other application sets they have permission to use.
When Citrix releases a new version of the ICA Client, Protection Insurance’s IT staff adds the client to the Client Update Database. When users initiate their connections to a MetaFrame XP server, the new ICA Client is “pushed” to their client devices. The MetaFrame XP administrator sets the update options to force users to disconnect from their ICA sessions and accept the updates. This ensures that all staff members are using the most current version of the ICA Client.

For more information about Client Auto Update, see “Updating the ICA Clients” on page 227 of this guide.
With MetaFrame XP, you can expand users’ access to information. You make information available to users by publishing applications and files on MetaFrame XP servers. You then decide whether users should open certain file types with these published applications or with applications running locally on client devices.

Using MetaFrame’s publishing capability, you can make the following types of resources available:

- Applications installed on MetaFrame servers. When users access them, the published applications appear to be running locally on client devices.
  
  You can publish any application that can run on the Windows console (32-bit Windows applications, 16-bit Windows applications, DOS applications, POSIX applications, and OS/2 applications).

- The MetaFrame server’s desktop, so users can access all of the resources available on the server.

- Data files such as Web pages, documents, sound files, spreadsheets, and URLs. In MetaFrame XP, the combined total of data types you can publish is referred to as content.

**Load Managed Applications**

If you are licensed for MetaFrame XPa or MetaFrame XPe, you can use Load Manager to publish an application to be hosted on multiple servers.

When a user connects to an application that is published on more than one server in the server farm, Load Manager determines where to start the ICA session based on server load.
You can adjust server load calculations for individual servers with Load Manager. For instructions about configuring load evaluators, see the *Load Manager Administrator’s Guide*, available in the Docs folder on the MetaFrame XP Server CD-ROM.

**Installation Manager Applications**

If you are licensed for MetaFrame XPe, you can install and publish Installation Manager packages for users to access. Using Installation Manager, you can simultaneously install an out-of-the-box application on all MetaFrame XP servers on your network from a single point without manual intervention.

Publishing an Installation Manager application causes each server that you specify to download and install the application. Deleting a published Installation Manager application uninstalls the application from each server that you specified to run the application.

For more information about using Installation Manager, see the *Installation Manager Administrator’s Guide*, located in the Docs directory on your MetaFrame XP Server CD-ROM.

**Using the Web Interface for MetaFrame XP to Present Applications**

If you want to provide users with access to published applications and content with a Web-based solution, you can use the Web Interface if you have a single MetaFrame XP server farm, or the Web Interface Extension if you have multiple server farms. For more information about these products, see the *Administrator’s Guide* for each of them. These guides are located in their respective Docs directories on the MetaFrame XP Components CD.

**Deciding How Users Access Information**

Before you begin publishing applications and content, review your network to identify obstacles that interfere with effectively managing resources. For example, you may encounter problems in the following areas:

- **Heavy server loads.** Users are viewing and downloading applications and files that consume a lot of bandwidth, which makes your network slow or unusable.
- **Security of servers and client devices.** Users frequently introduce viruses into the environment.
- **Desktop integrity.** Users damage client systems or make them unusable by misconfiguring them or by installing unauthorized or incompatible software.

To use MetaFrame XP to solve many of these types of problems, review the following questions:
• Which types of applications should users run on MetaFrame servers?
For example, if users introduce viruses and other destructive elements into the
network, publishing email applications, or perhaps all applications, for users to
access on MetaFrame XP servers can add a layer of protection.
If you prefer to have users run applications such as email programs locally, you
can use MetaFrame’s content redirection capability in conjunction with the ICA
Win32 Program Neighborhood Agent to redirect application launching from
client device to MetaFrame server. When users double-click email attachments
encountered in an application running locally, the attachment opens in an
application that is published on the MetaFrame server, associated with the
 corresponding file type, and assigned to the user.

• Which types of applications should users run locally on client devices?
For example, users may frequently access file types such as Web and
multimedia URLs when running published applications. Opening these file
types with Web browsers or streaming media players present on MetaFrame
servers can consume a lot of network bandwidth or result in heavy server load.
To free servers from processing these types of requests, you can redirect
application launching for supported URLs from the MetaFrame server to the
local client device.

• Which users should access applications locally and which should access
applications published on MetaFrame XP servers?
To provide a smoother user experience, review your user base, client hardware,
and client operating systems to determine which users should open which types
of applications.
For example, you may publish a financial spreadsheet on a MetaFrame server
for users in your accounting department to access. For security reasons, you
want these users to open the published file with the associated application
published on the MetaFrame server. However, you also published an audio file
of a keynote speech given by the company president. To prevent the MetaFrame
 servers from becoming overloaded, you want users to open this file with player
applications on their local client devices.

Managing Users’ Access to Information with Content Publishing
and Content Redirection

With MetaFrame’s capability to redirect application and content launching from
server to client or client to server, referred to as content redirection, access to
information is expanded even more. You decide whether users access information
with remote applications published on MetaFrame servers or with applications
running locally on client devices.
Content redirection provides flexibility when considering application management and information storage locations and allows you to more effectively manage all of the resources available in the enterprise. You can also use this capability if your users connect to resources published on MetaFrame XP servers through the Web Interface.

You can use the following methods, or combination of methods, to broaden information access:

- **Use content publishing** to provide access to document files, media files, Web pages, and any other type of file, regardless of storage location. Shortcuts to the published content are presented to users the same way shortcuts to published applications are presented.
  
  You can decide whether users open published files with local applications or with remote applications published on MetaFrame XP servers.
  
  For more information about publishing content, see “Publishing Content” on page 258.

- **Use content redirection** to redirect application launching from server to client or client to server. If a user receives an email attachment in a locally running email program, you can use content redirection to allow the attachment to be opened in a remote application published on a MetaFrame server. You can also allow users to open any Web and multimedia content they encounter while running a published application with local players, freeing server resources.
  
  You can determine which applications — remote or local — users launch in which situations.
  
  For more information about content redirection, see “Configuring Content Redirection” on page 255.

### Publishing Applications and Content

When you publish applications, you make applications that are installed on a MetaFrame XP server easily available to users. Similarly, you publish content to make documents, media files, URLs and other files available to users.

With application publishing, you can:

- Increase your control over application deployment
- Shield users from the mechanics of the Windows server environment
- Push application icons and shortcuts to user desktops through Program Neighborhood and the Program Neighborhood Agent

Use the Management Console to publish applications. With the Management Console, you can publish applications on any server in the MetaFrame XP server farm, including servers that are temporarily out of operation.
User Access to Published Applications

When you publish applications, user access to those applications is simplified in several areas.

**Addressing.** Instead of connecting to a MetaFrame XP server by its IP address or server name, users can connect to a specific application by whatever name you give it. Connecting to applications by name eliminates the need for users to remember which servers host which applications.

**Navigation.** Instead of requiring users to navigate the Windows interface on MetaFrame XP servers to find and start installed applications, users can connect directly to published applications.

**User authentication.** Instead of logging on to and logging off from multiple MetaFrame XP servers to access applications, Program Neighborhood users can be authenticated once to all servers in a server farm and get immediate access to all applications configured for their user group or specific user names.

Publishing applications for the special Citrix Anonymous user group lets you completely eliminate the need for user authentication for those applications you want to provide to all users on your network. For more information, see “Anonymous Users” on page 248.

Published applications are presented to users running the ICA Win32 Program Neighborhood Client as application sets. An application set is a user’s view of the resources published on MetaFrame XP servers that the user is authorized to run.

**Note** Users running the ICA Win32 Program Neighborhood Client open the Program Neighborhood interface to connect to applications and content published on MetaFrame XP server farms. The Program Neighborhood Client runs on Windows NT 4.0 Workstation, Windows 95, Windows 98, Windows Me, Windows 2000, and Windows XP platforms.

Publishing applications in your server farm benefits users of most ICA Clients. Although the UNIX, Macintosh, DOS, and Web Clients do not support the complete (server- and client-side) administrative configuration of the ICA connection provided by Program Neighborhood, these ICA Clients do support connections to published applications.

With the ICA UNIX, Macintosh, and DOS Clients, users benefit from application publishing’s simplified addressing and desktop navigation when they configure connections to published applications using their connection configuration managers.
With the ICA Clients that work with Web browsers (which are available as an Internet Explorer Active-X control, Netscape plug-in, or Java applet), you can create Web access that lets users click a link in a Web page to start a published application. You can use the Web Interface or Web Interface Extension for MetaFrame XP, or the application launching and embedding process to achieve this.

Setting up a Pass-Through ICA Client

When you run MetaFrame XP Setup, you can install the pass-through ICA Win32 Client on the server. You can install the full ICA Win32 Program Neighborhood Client or the Program Neighborhood Agent.

Install the pass-through ICA Win32 Program Neighborhood Client if you want to give users who run other ICA Clients access to the features of Program Neighborhood. Users launch Program Neighborhood from the server desktop or as a published application. When users connect to the Program Neighborhood published application, they can launch all other applications published on the MetaFrame XP servers in your farm from a single interface.

Install the pass-through ICA Win32 Program Neighborhood Agent if you want to give users who run other ICA Clients transparent access to published applications from the server desktop. When you use the pass-through Program Neighborhood Agent, links to published applications appear in the Start menu and the Windows System Tray and shortcuts appear on the server's desktop. Users can launch published applications from the server desktop; they do not have to open the Program Neighborhood interface.

Administrative Control of Applications

When you publish applications, you get greater administrative control over application deployment with:

**Selected user access.** You publish applications for specific users and user groups. By definition, an application you publish for a specific user group is unavailable to other groups.

**Enabled and disabled applications.** You can temporarily restrict all access to an application by disabling it. You can enable the application later to return access to users. This capability is useful when you want to take an application offline for maintenance.

**Multiple-server application hosting.** Application publishing, when used in conjunction with Load Manager, lets you direct ICA Client connection requests to the least busy server in a farm of servers configured to run an application.
Using Published Applications

When you publish an application, configuration information for the application is stored in the data store for the server farm. The configuration information includes which types of files are associated with the application; properties of the ICA connection, including its name; users who can connect to the application; and client-side session properties that include window size, number of colors, level of encryption, and audio setting.

To users, published applications appear very similar to applications running locally on the client device. The way users start applications depends upon which ICA Client they are running on the client device.

ICA Win32 Program Neighborhood Client. After starting Program Neighborhood, users find a list of applications, called an application set, published for their user account or user group.

ICA Client users on UNIX, Macintosh, and DOS. Using connection managers, these users can browse a list of all applications published on the network and select an application to run.

Web access. Users who have the ICA Win32 Web Client or the ICA Java Client can access applications using their Web browsers. You can use the Web Interface for MetaFrame XP or the application launching and embedding process to present hyperlinks to published applications. When users click these links, the published application or content is launched on the MetaFrame server. For more information about application launching and embedding, see “Deploying ICA Clients to Users” on page 219.

The ICA Win32 Program Neighborhood Agent integrates hyperlinks to published applications into the Windows desktop. You must use the Web Interface to allow users to connect using the Program Neighborhood Agent. For more information about using the Program Neighborhood Agent, the ICA Win32 Web Client, or the Program Neighborhood Client, see the ICA Win32 Client Administrator’s Guide, located in the IcaClientDoc directory on the Components CD-ROM included in your MetaFrame XP box.
For information about configuring Web access with the Web Interface, see the *Web Interface Administrator’s Guide*, located in the Docs directory on your MetaFrame XP Server CD-ROM.

## Configuring User Access to Applications

Before you publish applications, consider the network account authority that you use, and the ways that the configuration of your users’ accounts can affect user access to applications.

For general information about user account configuration, including use of Windows NT domains, Windows Active Directory, and Novell Directory Services (NDS), see “Network Configuration and Account Authority Issues” on page 66.

Publishing applications in MetaFrame server farms lets you set up two types of application access: explicit user account access and anonymous access.

### Anonymous Users

During MetaFrame XP installation, Setup creates a special user group named *Anonymous*. By default, this user group contains 15 user accounts with account names in the form Anon\(x\), where \(x\) is a three-digit number from 000 to 014. By default, anonymous users have guest permissions.

| Note | The total number of users, whether anonymous or explicit, who are logged on to a MetaFrame server farm at the same time cannot exceed the total license count of all the MetaFrame XP connection licenses in the server farm. |

| Note | MetaFrame XP cannot create anonymous user accounts on Windows primary or backup domain controllers. Therefore, you cannot publish applications for anonymous access on a MetaFrame XP server if it is a domain controller. Citrix does not recommend installing MetaFrame XP on Windows domain controllers. |

If an application you publish on a MetaFrame XP server can be accessed by users with guest permissions, you can configure the application using the Management Console for MetaFrame XP to allow access by anonymous users.

When a user starts an application that is configured for anonymous users, the server does not require an explicit user name and password to log the user on to the server and run the application.

Anonymous users are granted minimal ICA session permissions, which include the following properties that differ from standard ICA session permissions for the default user:
Ten-minute idle (no user activity) time-out
Log off from broken or timed-out connections
No password is required
The user cannot change the password

When an anonymous user session ends, no user information is retained. The server does not maintain desktop settings, user-specific files, or other resources created or configured for the ICA Client.

For more information about configuration of ICA connections on MetaFrame XP servers, see “Configuring ICA Connections” on page 195.

Configuring Anonymous User Accounts

The anonymous user accounts that MetaFrame XP creates during installation do not require additional configuration. If you want to modify their properties, you can do so with the standard Windows user account management tools.

Explicit Users

An explicit user is any user who is not a member of the Anonymous group. Explicit users have user accounts, which you create, configure, and maintain with standard user account management tools.

Explicit users who log on to MetaFrame XP server farms to run applications have a persistent existence: their desktop settings, security settings, and other information is retained between ICA sessions in a specific user profile.

Important: Do not assign any explicit users to the Anonymous group.

Procedures for Publishing Applications

Making applications and content available to users is an integral function of MetaFrame XP. Use the Management Console for MetaFrame XP to publish applications on any server in the farm to which you log on. You do not have to run the Management Console from the MetaFrame XP server on which the applications are installed. The server or servers hosting a published application must be a member of the server farm.

To publish an application

1. Open the Management Console for MetaFrame XP.
2. Verify that the server you want to host the application is a member of the server farm. You can find the intended host server or servers under the Servers object.
3. From the Actions menu, choose New > Published Application.

4. Follow the instructions in the Application Publishing wizard. Detailed help for each step is available by clicking Help.

Tip If you want to publish an application on additional servers, you can drag the application in the console tree and drop it on MetaFrame XP servers to publish the application on the servers. The application must already be installed on the servers, and it inherits its settings from the first server where you published the application.

Associating Published Applications with File Types

When you publish applications on MetaFrame XP servers, you can associate the published applications with certain file types present in the server’s Windows registry.

Associate published applications with file types to:

- Implement Content Redirection from client to server for users running the ICA Win32 Program Neighborhood Agent
- Have users open content published on MetaFrame XP servers with applications published on MetaFrame XP servers

Important If you install and then publish applications after installing MetaFrame XP, you must update the file type associations in the server’s Windows registry. For instructions for doing this, see “Updating File Type Associations in the Server Farm” on page 252.

When you associate published applications with file types and then assign the applications to users, you automatically implement the following:
1. Users running the ICA Win32 Program Neighborhood Agent open all files of the associated type encountered in locally running applications with applications published on the MetaFrame XP server.

For example, when users double-click email attachments encountered in an application running locally, the attachment opens in an application that is published on the MetaFrame server, associated with the corresponding file type, and assigned to the user. This feature is named Content Redirection from client to server.

If you do not want this to occur for any Program Neighborhood Agent users, do not associate the published application with any file types. If you do not want this to occur for specific Program Neighborhood Agent users, do not assign those users to the published application associated with the file type.

For more information about Content Redirection, see “Configuring Content Redirection” on page 255.

2. Users connecting through the Web Interface or using the Program Neighborhood Agent open published content of the associated file type with the application published on the MetaFrame server.

For example, you publish a document of the Microsoft Word for Windows type. This feature is named Content Publishing. When you also publish the Microsoft Word application, associate it with a list of file types (files with the .doc extension, for example), and assign it to a group of users, the published content is opened in the Microsoft Word application published on the MetaFrame server. This occurs for users when they log on to the Web Interface logon page and click the link to the published content (the document, in this case).

If you do not want this to occur for any users, do not associate the published application with any file types. If you do not associate the published application with any file types, users open the published content with local player or viewer applications if they are installed on the client devices.

For more information about Content Publishing, see “Publishing Content” on page 258.

You associate published applications with file types on the last page of the Publishing wizard or on a published application’s property page.

Depending on how or if you want to redirect application launching, you may need to publish the same application more than once. Follow the procedures below to associate published applications with file types:

- **To associate a published application with file types when running the Publishing wizard**

  1. Open the Management Console for MetaFrame XP.
  2. If you have not yet published the application, select **New > Published Application** from the Actions menu.
3. Follow the instructions on the pages of the Publishing wizard. For detailed online help, click Help on each page.

4. On the last page of the wizard, select the file types you want to associate with the published application.

**Note** When you associate a file type with a published application, several file extensions can be affected. For example, when you associate the Word document file type, file extensions in addition to the .doc extension are associated with the published application.

5. Click **Finish** when you are done.

To associate a published application with file types for an application you already published

1. Open the Management Console for MetaFrame XP.
2. Expand the Applications node in the left pane to display your published applications.
3. Right-click the application you want to associate with file types and choose **Properties** from the short-cut menu that appears.
4. On the **Content Redirection** tab, select the file types you want to associate with the published application.

**Note** When you associate a file type with a published application, several file extensions can be affected. For example, when you associate the Word document file type, file extensions in addition to the .doc extension are associated with the published application.

5. Click **OK** when you are done.

**Updating File Type Associations in the Server Farm**

You can verify which file types are associated with a published application on an application’s property sheet. You can view all file types associated with published applications for the entire server farm on the **Content Redirection** tab, displayed when you select the server farm in the left pane of the console.

Follow the procedure below to update file type associations in your server farm. If you publish applications to be hosted on more than one server, be sure to update the file types for each server.
To update file type associations in the server farm
1. Open the Management Console for MetaFrame XP.
2. Expand the Servers node in the left pane.
3. Right-click a server and select Update File Types from Registry.

Passing Parameters to Published Applications

When you associate a published application with file types, MetaFrame XP
appends the symbols “%*” (percent and star symbols enclosed in double quotation
marks) to the end of the application’s command line. These symbols act as a
placeholder for client-passed parameters.

If a published application doesn’t launch when expected, verify that its command
line contains the symbols cited above. If you do not see these symbols in an
application’s command line, you can add them manually.

If the path to the application’s executable includes directory names with spaces
(such as Program Files), you must enclose the command line for the application in
double quotation marks. To do this, follow the instructions below for adding
quotation marks around the %* symbols and then add a double quotation mark at
the beginning and the end of the command line. Be sure to include a space between
the closing quotation mark and leave the double quotation marks around the percent
and star symbols.

For example, change the command line for the published application Windows
Media Player to the following:

C:\Program Files\Windows Media Player\mplayer1.exe” “%*”

The following procedures assume you want to add the symbols to the Notepad
application, which is published on a MetaFrame XP server.

To add a parameter placeholder to a published application
1. In the Management Console for MetaFrame XP, expand the Applications node.
   Select the application to use and choose Properties.
2. In the Properties dialog box, select the Application Location tab.
3. In the Command Line box, add a space and “%*” (percent and star symbols
   enclosed in quotation marks) to the end of the command line. For example, for
   the following command line:
   C:\Winnt\System32\Notepad.exe
   Add “%*” to the end, as follows:
   C:\Winnt\System32\Notepad.exe “%*”
4. Choose OK to save the changes.
Creating Files for Application Launching and Embedding

You can create the files you need to allow users to access published applications from a Web page. You must create two types of files — an HTML file and an ICA file — to enable users to do this. This process is called *Application Launching and Embedding*.

If you are using the Web Interface or Web Interface Extension for MetaFrame XP, you do not need to manually create these separate HTML and ICA files.

The Create HTML File wizard and the Create ICA File wizard walk you through creating these files. To launch one of these wizards, select a published application in the Management Console for MetaFrame XP and click the Create ICA File or Create HTML File buttons on the toolbar. The wizards walk you through the process of creating the necessary files.

Creating an ICA File

An ICA file contains published application information in Ini file format. You can create ICA files and distribute them to users. When users double-click ICA file icons, the published application is launched.

When a user receives an ICA file, the user’s client device initializes a session to run the specified application on the MetaFrame XP server.

- **To create an ICA file for an application**
  1. Select the published application in the Applications folder in the left pane of the Management Console. When you select an application, new menu options and toolbar buttons appear.
  2. Click the Create ICA File button on the toolbar or choose Application > Create ICA File from the Actions menu.
  3. Follow the instructions in the Create ICA File wizard to create your ICA File.

Creating an HTML File

You can easily create an HTML page that presents users with links to published applications. When users click the link in the HTML file you create, the connection is implemented through an ICA file. You can also create the ICA file when you generate the HTML file.

- **To create an HTML file**
  1. Select the published application in the Applications folder in the left pane of the console.
  2. Choose Create HTML File from the toolbar or the Actions menu.
3. Follow the instructions in the wizard to create your HTML file.

Removing Published Applications

As you publish updated applications on your servers, you can remove the older or less-used applications. Removing a published application does not uninstall the application from the MetaFrame XP server, or make it completely unavailable to ICA Clients. Removing a published application from the server farm simply stops advertising the application’s availability.

- **To remove a published application**
  1. Select the application you want to remove under **Applications** in the left pane of the Management Console for MetaFrame XP.
  2. From the **Actions** menu, choose **Delete Published Application**.
  3. When prompted, confirm the deletion by clicking **OK**.

Configuring Content Redirection

With Content Redirection, you determine which applications — remote or local — users launch and in which situations. Use Content Redirection to redirect application launching from:

- Client to server
- Server to client

Redirecting Content from Client to Server

When you configure **Content Redirection from client to server**, users running the ICA Win32 Program Neighborhood Agent open all files of the associated type encountered in locally running applications with applications published on the MetaFrame XP server. You must use the Web Interface to allow users to connect to published applications with the Program Neighborhood Agent.

- **Note**  Content Redirection from client to server is available only with MetaFrame XPa or MetaFrame XPe.

The Program Neighborhood Agent gets updated properties for published applications from the server running the Web Interface for MetaFrame XP. When you publish an application and associate it with file types, the application’s file type association is changed to reference the published application in the client device’s Windows registry.
If you have users who run applications such as email programs locally, you can use MetaFrame’s content redirection capability in conjunction with the ICA Win32 Program Neighborhood Agent to redirect application launching from client device to MetaFrame server. When users double-click attachments encountered in an email application running locally, the attachment opens in an application that is published on the MetaFrame server, associated with the corresponding file type, and assigned to the user.

**Important** You must enable client drive mapping to use this feature. You can enable client drive mapping for the entire server farm, for specific servers, or for specific users with user policies. For more information about user policies, see “Creating and Applying User Policies” on page 281.

If you do not want this to occur for any Program Neighborhood Agent users, do not associate the published application with any file types. If you do not want this to occur for specific Program Neighborhood Agent users, do not assign those users to the published application associated with the file type.

Follow the procedure below to configure Content Redirection from client to server.

**To configure Content Redirection from client to server**

1. Determine which of your users connect to published applications using the Program Neighborhood Agent. Content Redirection from client to server applies only to those users connecting with the Program Neighborhood Agent.
2. Verify that client drive mapping is enabled. You can enable client drive mapping for a specific connection using Citrix Connection Configuration or for specific users by creating user policies.
3. Publish applications you want the Program Neighborhood Agent users to open on the MetaFrame server.
4. When you publish the application, associate it with file types on the last page of the Application Publishing wizard.

**Redirecting Content from Server to Client**

When you enable **Content Redirection from server to client**, embedded URLs are intercepted on the MetaFrame server and sent to the ICA Client using the ICA Control virtual channel. The user’s locally installed browser is used to play the URL. Users cannot disable this feature.

For example, users may frequently access Web and multimedia URLs they encounter when running an email program published on a MetaFrame server. If you do not enable Content Redirection from server to client, users open these URLs with Web browsers or multimedia players present on MetaFrame servers.
To free servers from processing these types of requests, you can redirect application launching for supported URLs from the MetaFrame server to the local client device.

**Note** If the client device fails to connect to a URL, the URL is redirected back to the server.

The following URL types are opened locally on ICA Win32 and Linux Clients when this type of content redirection is enabled:

- HTTP (Hypertext Transfer Protocol)
- HTTPS (Secure Hypertext Transfer Protocol)
- RTSP (Real Player and QuickTime)
- RTSPU (Real Player and QuickTime)
- PNM (Legacy Real Player)
- MMS (Microsoft’s Media Format)

**Note** If Content Redirection from server to client is not working for some of the HTTPS links, verify that the client device has an appropriate certificate installed. If the appropriate certificate is not installed, the HTTP ping from the client device to the URL fails and the URL is redirected back to the server.

Content Redirection from server to client requires Internet Explorer Version 5.5 with Service Pack 2 on systems running Windows 98.

Follow the procedures below to enable Content Redirection from server to client.

1. **To enable Content Redirection from server to client**

   Determine if you want Content Redirection from server to client to apply for the entire server farm, for specific MetaFrame servers, or for specific users only.

   To apply the behavior to the entire server farm, select the farm in the Management Console for MetaFrame XP and then click Properties. Select **MetaFrame Settings** in the left pane of the farm’s Properties page. Select the option **Enable Content Redirection from server to client**.

   To apply the behavior to a specific server, select the server in the Servers node in the Management Console and then click **Properties**. Select **MetaFrame Settings** in the left pane of the server’s Properties page. Select the option **Enable Content Redirection from server to client**.
To apply the behavior to specific users, create a user policy and enable the rule **Content Redirection from Server to Client**. Assign the policy to only those users you want to open supported URL file types on client devices. For more information about user policies, see “Creating and Applying User Policies” on page 281.

**Publishing Content**

You can give users access to information, such as documents, Web sites, and video presentations, by publishing content for users in the same way that you publish applications in a MetaFrame XP server farm.

With content publishing, you can publish and manage various types of content and present it to users with the applications they need. Published content and published applications appear together through the Web Interface for MetaFrame XP, Program Neighborhood, and Program Neighborhood Agent interfaces.

You can configure MetaFrame to allow users to open published content in local player or viewer applications running on client devices or in applications published on MetaFrame servers.

**Publishing Content to be Opened with Applications Published on MetaFrame Servers**

Follow these basic steps if you want users to open published content with applications published on MetaFrame XP servers.

1. Publish the data file you want users to access. For more detailed instructions for publishing content, see “Publishing Content on MetaFrame XP Servers” on page 260.

2. Determine which users you want to open the published content with a published application.

3. Publish the application that corresponds to the content file type. For example, if you published a Microsoft Word for Windows document file named “Quarterly_Sales.doc,” publish Microsoft Word on a MetaFrame XP server. For more information about publishing applications, see the online Help for the Application Publishing wizard.

4. When you publish Word, associate the file type “Word document” with the application.
Note When you associate a file type with a published application, several file extensions can be affected. For example, when you associate the Word document file type, file extensions in addition to the .doc extension are associated with the published application.

5. Assign the published Word to the users you want to open the published document with the published application.

Publishing Content to be Opened with Applications on Local Client Devices

When you configure MetaFrame XP to allow users to open published content with applications running locally on client devices, the ICA Client passes the name of the published content file to the local viewer application. The MetaFrame XP server does not download the file to the ICA Client. Instead, the local viewer application accesses the file the same as it would if a user double-clicked the file in Windows Explorer (and a file type association specified the application to use).

For example, when a user opens a published Microsoft Streaming Media file in Program Neighborhood, the Windows Media Player application runs on the client device to play the content. You can publish any content for users to view with a local viewer application.

Publishing content does not use ICA Client or MetaFrame XP server resources or licenses, because local viewer applications do not use ICA sessions to display the published content.

Follow these basic steps for publishing content for users to access with applications running locally on client devices.

1. Publish the data file you want users to access. For more detailed instructions for publishing content, see “Publishing Content on MetaFrame XP Servers” on page 260.

2. If you happen to publish the application that corresponds to the content file type, do not associate it with any file types if you want all users to open the published content with locally installed applications.

However, if you want some users to open the published content with the published application, you can associate the published application with the content file type, but only assign the application to those users. For more information about publishing applications, see the online Help for the Application Publishing wizard.
Content Publishing Requirements and Limitations

The following requirements and limitations apply when publishing content in MetaFrame XP server farms:

- You can publish content using the Management Console for MetaFrame XP when a server farm is in mixed mode for interoperability with MetaFrame 1.8. However, users do not see published content in Program Neighborhood, Program Neighborhood Agent, or the Web Interface if the MetaFrame XP server farm is in mixed mode.

- Published content appears in application sets in Program Neighborhood, Program Neighborhood Agent, and the Web Interface, so access to published content requires that the ICA Client support those features. You cannot create custom ICA connections to access published content.

- You cannot publish a UNC directory path to display a folder to users of Netscape Navigator versions prior to 6.0. See “Specifying Locations for Publishing Content” on page 261 for more information.

- When you publish a file using a network path, users must have permission to access the file on the network to be able to access it as published content through MetaFrame XP.

Publishing Content on MetaFrame XP Servers

You publish content using the Management Console for MetaFrame XP and the Publishing wizard. You can select options in the wizard when you publish content, and you can later check and modify the settings in the Properties dialog box for the published content.

If you want users to open published content with local applications, the applications must be associated with published content through Web browser MIME types or Windows file associations on the client device. No other client-side configuration is necessary after viewer applications are installed and associations are configured.

To publish content

1. In the Management Console for MetaFrame XP, choose Actions > New > Published Application to open the Publishing wizard. Enter the information requested in the wizard and select the options you want to use. To move between pages, click Next to continue or Back to return to a previous page.

2. Type a name for the content you are publishing in the Display Name box. This text appears as the name of the icon that represents the published content.

3. When the wizard asks what you want to publish, select Content.
4. In the **Content Address** box, specify the location of the content by entering a URL or UNC address. See “Specifying Locations for Publishing Content” below for more information.

5. After specifying the content address, continue using the wizard to specify other settings and publish the content.

**Specifying Locations for Publishing Content**

When you publish content, you can specify the location using a variety of address formats. You can enter any of the following types of information (examples shown in parentheses):

- **HTML Web site address**  (http://www.citrix.com)
- **Directory on an FTP server**  (ftp://ftp.citrix.com/metaXP)
- **UNC file path**  (file://myServer/myShare/myFile.asf) or (\myServer\myShare\myFile.asf)
- **UNC directory path**  (file://myServer/myShare) or (\myServer\myShare)

*Important* Specifying a UNC directory path does not correctly display the specified directory to users of Netscape Navigator prior to Version 6.0. Earlier versions of Navigator incorrectly interpret the path as relative to the Web server. To publish a directory to such users, consider specifying an FTP directory or listable Web server directory.

**Setting CPU Priority Levels for Applications**

By default, MetaFrame XP gives all published applications equal priority for access to CPU cycles. All application instances run with normal CPU priority.

The default configuration assumes that CPU access by all applications is equally important. The default configuration does not prevent one application from consuming resources that are required by other, mission-critical applications running on the same server.
You can manage some aspects of resource usage by applications through your deployment methods. For example, you can isolate mission-critical applications by publishing them on separate servers so less-important applications do not compete for server resources. You achieve better performance by publishing CPU- and memory-bound applications on high-performance servers.

MetaFrame XP provides a setting you can apply to published applications to prioritize their CPU access. You can use the CPU priority settings on servers running Windows server operating systems.

**Note** The term *published application* in this section refers to applications and MetaFrame XP server desktops that are published for users in the server farm. It does not refer to published content such as documents and media files.

You can apply a CPU priority setting to each published application. Each instance of the application that runs in the server farm is affected by the setting. When multiple servers host the same published application, the setting applies to each server on which the application runs in the server farm.

If you publish the same application more than once—for separate groups of users, different host servers, or with different settings, for example—you create separate published applications; each can have its own CPU priority setting.

You can use this setting in any size server farm, independent of load management features in MetaFrame XPa and MetaFrame XPe. Load management distributes connections to MetaFrame servers based on the servers’ loads. In contrast, the CPU priority setting applies to a published application that runs on any server in the server farm.

**Assigning CPU Priority Levels to Applications**

When you assign a CPU priority level to a published application, the priority level that you specify is used by the CPU scheduler on all servers that host the published application (and for every instance of the application that runs on a server). When a server is executing multiple applications, the CPU scheduler prioritizes CPU access by application threads according to the priority level that you assign or the default priority level.

With this option, you can assign normal or lower CPU priority to Microsoft Internet Explorer, for example, and assign high CPU priority to an application whose performance is more important to the enterprise, such as PeopleSoft Human Resources Management. A higher priority setting gives Human Resources Management a performance advantage over Internet Explorer when both applications run on the same server.
You can assign five priority levels (in order from lowest to highest priority): low, below normal, normal, above normal, and high. The default is normal.

**Important** High priority indicates a process that performs time-critical tasks. The threads of a high-priority process preempt the threads of low- and normal-priority processes. An example is the Task List, which must respond quickly when called by the user, regardless of the load on the system. Use extreme care when using the high-priority setting. A CPU-bound application assigned high priority can consume nearly all available CPU cycles, which can cause unacceptable performance by other applications running on the server.

The CPU priority option is in the Application Publishing wizard and on the **Application Limits** page in the **Properties** sheet for each published application. You can set the priority level when you first publish applications and set or change the level for published applications using the Management Console for MetaFrame XP.

- **To publish an application and set its CPU priority**
  1. In the Management Console, choose **Actions > New > Published Application** to run the Application Publishing wizard.
  2. Proceed through the wizard pages, entering information and selecting options for the application you are publishing.
  3. Select an option from the **CPU priority level** menu. The default setting is Normal.
  4. Click **Next** and then proceed through the subsequent screens until you complete the wizard’s steps.

- **To modify the CPU priority of a published application**
  1. In the Management Console’s left pane, expand the Applications node. Select the application you want to modify and choose **Properties**.
  2. In the **Properties** sheet, click **Application Limits** in the left pane.
  3. Select an option from the **CPU priority level** menu. The default setting is Normal.
  4. Click **OK** to apply the setting and close the dialog box.
Managing Users and ICA Sessions

This chapter describes how to manage users and their ICA sessions in a MetaFrame XP server farm. It includes information about using the Management Console for MetaFrame XP and Citrix Web Console to monitor users’ connections. This chapter also includes information about creating and applying user policies to control select MetaFrame XP settings for users or user groups.

You can perform session-management activities, including logging off, shadowing, disconnecting, and sending messages to users, using either the Management Console or Citrix Web Console. Some management and monitoring activities can be performed only in the Management Console. For more information about the Management Console, see “The Management Console for MetaFrame XP” on page 173. For more information about Citrix Web Console, see “Citrix Web Console” on page 181.

**Note** You may not see some or all of the data described below if you have not been granted permission to perform these tasks. See your primary MetaFrame XP administrator for more information.

### Controlling User Logons

You can control the ability of users to establish sessions on the MetaFrame XP servers in a server farm by enabling or disabling logons. By default, logons are enabled when you install MetaFrame XP. You might want to disable logons when you install software or perform other maintenance or configuration tasks.

- **To enable or disable logons**
  1. Right-click a server in the tree in the Management Console for MetaFrame XP and choose Properties to display the Properties page. Select MetaFrame XP Settings in the left pane.
2. To prevent users from logging on, make sure Enable logons to this server is not selected on MetaFrame XP Settings.

To restore the ability of users to connect to the server, select Enable logons to this server.

**Controlling User Connections**

When user logons are enabled, MetaFrame XP does not limit user access to ICA sessions and published applications. In general, users can launch multiple connections and can connect to any published application that they are authorized to use.

You can use the connection control feature to control connections to MetaFrame XP servers and published applications. This feature can help you maintain availability of resources in a server farm.

Having no limit on connections works best in an environment where users and published applications are well-behaved. All users have equal access to the published applications.

Adverse usage conditions in a server farm can degrade performance and reliability. In an unregulated environment, you might encounter the following problems:

- Errors caused by individual users who run more than one instance of a published application at the same time.
- Denial-of-service attacks by malicious users who run multiple application instances that consume server resources and connection license counts.
- Over-consumption of resources by non-critical activities such as Web browsing.

Connection control provides two types of limits, as shown in the following table.

<table>
<thead>
<tr>
<th>Limit type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Concurrent connections in the server farm</td>
<td>Restricts the number of concurrent connections (ICA sessions) that each user in the server farm can establish. See “Limiting Total Connections in a Server Farm” on page 267.</td>
</tr>
<tr>
<td>Published application instances</td>
<td>Restricts the total number of instances of a published application that can run in the server farm at one time, and prevents users from launching more than one instance of a published application. See “Limiting Application Instances” on page 267.</td>
</tr>
</tbody>
</table>
Chapter 11 Managing Users and ICA Sessions

Limiting Total Connections in a Server Farm

When a user launches a published application, the ICA Client establishes a connection to a MetaFrame XP server and initiates an ICA session. If the user launches a second published application (without logging off from the first one), this creates a second concurrent connection in most cases.

Note The seamless session option in the ICA Client enables session sharing, a mode in which more than one published application runs with a single connection. If a user runs multiple applications with session sharing, the session counts as one connection.

To conserve resources, you can limit the number of concurrent connections that users are permitted to establish. The limit applies to each user who connects to the server farm. A user’s active sessions and disconnected sessions are counted for the user’s total number of concurrent connections.

For example, you can set a limit of three concurrent connections for users. If a user has three concurrent connections and tries to establish a fourth, the limit you set prevents the additional connection. A message tells the user that a new connection is not allowed.

Limiting connections can help you maintain availability of ICA connection license counts as well as prevent over-consumption of server resources by a few users.

You can apply the concurrent connections limit to all users, including members of the local administrators group. To set connection limits, select Connection Limits in the left pane of the farm’s Properties page.

Note The option Enforce limit on administrators refers to local administrators. By default, local administrators are exempt from the limit so they can establish as many connections as necessary.

Limiting Application Instances

By default, users in a server farm have unlimited access to the published applications that they are authorized to use. MetaFrame XP servers do not limit the number of instances of a published application that can run at one time in a server farm. Also, by default, a user can launch more than one instance of a published application at the same time.

With connection control, you can specify the maximum number of instances of a published application that can run at one time in the server farm.
For example, you can publish Autodesk AutoCAD and set a limit of 30 concurrent instances in the server farm. When 30 users are running AutoCAD at the same time, no more users can launch the application because of the limit of 30 concurrent instances.

Use the concurrent instances limit to enforce an application’s licensing requirement, for example.

Another connection control option lets you prevent any user from running multiple instances of a particular published application. With some applications, running more than one instance in a single user context can cause errors on the server.

You can apply application limits independently to each published application. For example, you can apply the limitations on total concurrent instances and multiple instances by a single user to one published application. You can limit only the total concurrent instances of another application. You can configure a third application to limit launching of multiple instances by individual users.

**Configuring Connection Control Settings**

You can use connection control to manage published applications and published desktops only. Connection control options do not apply to published content such as documents and media files, which execute on the client device. For more information about publishing content, see “Making Information Available to Users” on page 241.

Connection control is implemented entirely on MetaFrame XP servers. The ICA Client contains no configuration options related to connection control. Connection control affects users only if a connection attempt is prevented. If a user’s connection exceeds a connection limit, the client displays a message that describes why the connection is not available.

You configure connection control settings, including the option to log events related to connection control, in the Management Console.

The option to limit each user’s total concurrent connections in the server farm is available from **Connection Limits** on the **Properties** page for the server farm.

Options for limiting application instances are available when you select **Application Limits** in the left pane of each application’s **Properties** page. You can also set these options when you publish an application.

- **To limit concurrent connections in a server farm**

  Use this procedure to set the number of concurrent connections that each user can establish in the server farm.

  1. In the Management Console, right-click the farm node and choose **Properties**.
  2. In the **Properties** page, select **Connection Limits**.
3. Select **Maximum connections per user** to limit each user’s concurrent connections. Enter the number of concurrent connections to allow for each user.

4. If you want the connection limitation to apply to everyone, including local administrators, select **Enforce limit on administrators**.

5. Click **OK** to apply the settings and close the page.

- **To publish an application or desktop with application limits**
  1. In the Management Console, choose **Actions > New > Published Application** to run the Application Publishing wizard.
  2. Proceed through the wizard pages, entering information and selecting options for the application you are publishing.
  3. Under **Concurrent Instances**, select one or both of the following options:
     - **Limit instances allowed to run in server farm**. Select this option and enter the maximum number of instances that can run at one time in the server farm (without regard to who launches the application).
     - **Allow only one instance of application for each user**. Select this option to prevent any user from running more than one instance of this application at the same time.
  4. After you enter all required information and select the options to use, click **Finish** to publish the application.

- **To set application limits on a published application or desktop**
  1. In the Management Console, right-click the published application or desktop and choose **Properties**.
  2. In the **Properties** page, select **Application Limits**.
  3. Configure the following options:
     - **Limit instances allowed to run in server farm**. Select this option and enter the maximum number of instances of this application that can run in the server farm at one time.
     - **Allow only one instance of application for each user**. Select this option to prevent each user from running more than one instance of this application at the same time.
  4. Click **OK** to apply the settings and close the page.
Logging Connection Control Events

You can enable logging for connection control events when you select **Connection Limits** in the left pane of the farm’s **Properties** page. By default, event logging is disabled.

Event logging records an entry in the System log each time a server denies a user connection because of a connection control limit. Each server records the data in its own System log.

The following limits can result in connection denials, which the system records if logging is enabled.

**Maximum connections per user.** You can limit users to a maximum of five connections, for example. If a user tries to launch a sixth connection, the server denies the connection request and records the user’s name and the time in the System log.

**Application instances.** You can limit a published application to a certain number of concurrent instances. If you type 10 in **Maximum instances** and a user tries to launch the application when 10 instances are running, the server denies the connection request and records the user name, the time, and the name of the published application in the System log.

Use **Limit instances allowed to run in server farm** on **Application Limits** in the **Properties** page to limit instances of each published application.

**Application instances per user.** You can configure a published application to allow each user to run only one instance of the application. If a user tries to launch a second instance of the application, the server denies the connection request and records the user name, the time, and the name of the published application in the System log.

Use **Allow only one instance of application for each user** on **Application Limits** of the **Properties** page to limit each published application to one instance for a user.

To enable logging of connection control events

1. Right-click the farm node in the Management Console and choose **Properties**.
2. In the **Properties** page, select **Connection Limits**.
3. Select **Enable logging of over-the-limit denials**.
4. Click **OK** to apply the setting and close the page.
Monitoring and Managing ICA Sessions

You can use the Management Console and Citrix Web Console for monitoring and management of your user’s ICA sessions. You can use the consoles to:

- Monitor ICA sessions according to the published applications and MetaFrame XP servers to which they are connected
- Send messages to users in active ICA sessions
- Reset or disconnect sessions and log off users
- Use shadowing to monitor and remotely control selected sessions

This section describes how to use the Management Console for session monitoring and management. If you need help performing these actions in Citrix Web Console, click the Help button that is displayed in the Web console.

Viewing Information about ICA Sessions

Several tabs in the Management Console for MetaFrame XP display information about ICA sessions in table format. Each row in the table lists details for one ICA session. You can use different views in the console to monitor user sessions based on the published applications that users are connected to, or the servers where the ICA sessions are established.

Active sessions appear on several tabs when a MetaFrame XP server has active ICA Client sessions:

- When you select a published application in the tree, sessions that are running the application appear on the Users tab
- When you select a server, sessions that are running on the server, including console sessions, appear on the Users and Sessions tabs
- When you select the Servers node in the tree, the Users tab displays sessions running all servers; console sessions do not appear on this tab
For example, if you select a published application, the **Users tab** in the right pane displays the sessions in which the selected application is running. The information appears in columns, which display the user name, client device name, session ID number, server name, session, the state of the session, and the time the user logged on.

### Session Information Displayed in the Console

On the tabs that display ICA session information, each row represents one ICA session. You can click the column headings to sort the information. When you click the active sort heading, you reverse the sort order. You can rearrange the information in the table by dragging a column heading to a new position.

The session information that appears in the console includes details that help you identify the various types of sessions and the users associated with the sessions. The following column labels appear on tabs that display session information.

**User.** The name of the user account that initiates a session appears in the User column for each session. In the case of anonymous connections, the user name is a string with the letters “Anon” followed by a session number.

**Server.** The MetaFrame XP servers on which the selected application is running appear in this column.

**Session.** The Session column identifies a session with a name that includes the protocol that the session uses, usually ICA or RDP (for Microsoft’s Remote Display Protocol). The name also includes the network protocol for the session, and a number that distinguishes the session from other sessions that are running on the server.
**Session ID.** The Session ID is a unique number that begins with 0 for the first connection to the console. Listener sessions are numbered from 65,537 and numbered backward in sequence.

**State.** A session’s state is listed as Active, Listen, Idle, Disconnected, or Down. The meaning of session state labels is explained in the following section, which describes commands you use for managing sessions on MetaFrame XP servers.

**Type.** The type of connection being used to connect to the server, ICA or RDP, for example.

**Client name.** This column displays the name of the client device that is running the session.

**Application.** The name of the published application running within this session.

**Logon Time.** The time at which the user logged on.

**Idle Time.** The amount of time during which the user has not interacted with the application.

### Using Session Management Commands

In the Management Console for MetaFrame XP and Citrix Web Console, you can select ICA sessions and choose commands to manage the sessions.

In the Management Console, use the **Actions** menu and the toolbar buttons to choose session management commands. You can right-click a session in the console and choose commands from the menu that appears.

In Citrix Web Console, session-management commands are available when you select a session by clicking the check box to the left of the User name.

<table>
<thead>
<tr>
<th>Sessions</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>All Sessions</strong></td>
</tr>
<tr>
<td><strong>User</strong></td>
</tr>
<tr>
<td>[ ]</td>
</tr>
</tbody>
</table>

To display session information, click the Session link on the left of the Web console page.
Disconnecting ICA Sessions

To disconnect an ICA session, choose Disconnect. When you disconnect a session, you close the connection between the ICA Client and the MetaFrame XP server. However, this does not log off the user, and programs that were running in the session are still running on the server. If the ICA Client user then connects to the server (by selecting a published application or custom connection to the server), the disconnected session is reconnected to the client.

Connecting to Disconnected Sessions

When an ICA session is disconnected, the word “Disconnected” appears in the State column on the tabs in the Management Console where session information appears.

You can connect to a user’s disconnected session by choosing Connect. Your session must be capable of supporting the video resolution of the disconnected session. From the system console, you can connect only to sessions that were disconnected from the console.

Shadowing ICA Sessions

If you enabled shadowing on the server when you installed MetaFrame XP, you can shadow a user’s ICA session. Shadowing allows you to view the user’s actions and take remote control of the user’s keyboard and mouse. See “Using Shadowing to Monitor ICA Sessions” on page 209 for more information about shadowing.

Sending Messages to Users

You can send a message to a user by selecting the user’s sessions and choosing Send Message. You can select multiple sessions to send a message to multiple users at the same time. For information about viewing sessions, see “Viewing Information about ICA Sessions” on page 271.

To broadcast a message to all users, you can select all active user sessions in the right pane in the console.

In the Send Message dialog box, you can type a message title; the user name of the MetaFrame XP administrator who is logged on to the console and the current time appear in the Title box by default. Type the message text in the Message box. The text you type automatically wraps to the next line if you type past the right margin.

When you finish typing the message, click OK to send the message to the selected sessions. (In Citrix Web Console, click Send Message to send the message.)
Chapter 11 Managing Users and ICA Sessions

Resetting ICA Sessions

Resetting a session with the Reset command terminates all processes that are running in that session. You can use the Reset command to remove remaining processes in the case of a session error. However, resetting a session can cause applications to close without saving data.

If you reset a disconnected session, the word Down appears in the State column for the session. When you refresh the console display or when the next automatic refresh occurs, the session no longer appears in the list of sessions.

Resetting All Sessions

Special sessions that listen for requests to connect to the server are identified by the word Listen in the State column. If you reset a listener session, the server resets all sessions that use the protocol associated with the listener. For example, if you reset the ICA listener session, you reset the ICA sessions of all users who are connected to the server.

Viewing ICA Session Status

You can use the Status command to display user and I/O information about a session. The Session Status dialog box displays connection statistics, including the count of incoming and outgoing data that is transmitted in the session and the number of errors and the compression ratio used in the session. The dialog box also shows the user name and session name.

By default, the Session Status data is updated every second. You can choose the command buttons in the dialog box to reset the counters and refresh the data.
• Click **Reset Counters** in the dialog box to return all counters to zero.
• Click **Refresh Now** to immediately refresh the displayed data.

**Logging Off ICA Sessions**

Choose **Logoff Selected Session** to force a user’s session to end. If you select multiple sessions, choosing the command ends each selected session.

---

**Important**  Ending users’ sessions with the **Logoff Selected Session** command can result in loss of data if users do not close their applications first. You can send a message to warn users to exit all applications if you need to log off their sessions.

---

**Viewing Session Details**

You can select a session in the Management Console for MetaFrame XP and choose **Session Information** to view detailed information about the processes, settings, ICA Client software, and client cache associated with the selected ICA session.

**Viewing and Terminating Processes**

If you need to terminate a process started by an ICA session, select an ICA Client session and select the **Processes** tab in the right pane of the console. You can right-click a process and choose the **Terminate** command to terminate the process.

---

**Reconnecting ICA Sessions Automatically**

If users are disconnected from their ICA sessions because of unreliable networks, highly variable network latency, or range limitations of wireless devices, the result is lost productivity for users who must manually reconnect to their applications. Unreliable connections, such as WAN links, frequently cause time-out of TCP retransmission, which can cause loss of an ICA connection.

With the **auto client reconnection** feature, an ICA Client can detect broken ICA connections and automatically reconnect users to disconnected sessions. When this feature is enabled, users do not have to reconnect manually to continue their work.

The ICA Clients for Win32, WinCE, and Java support auto reconnect for ICA sessions over TCP. Auto reconnect does not work with sessions embedded in applications using the ICA Client Object.
How Automatic Reconnection Works

When the ICA Client detects an unintended disconnection of an ICA session, the client attempts to reconnect to the session until there is a successful reconnection or the user cancels the reconnection attempts.

ICA sessions using a connection that breaks can remain active. Users can reconnect only to sessions that are in a disconnected state. Cookies containing keys to user credentials and session IDs are created on the client device when ICA sessions are started. Because users can be reconnected only to disconnected sessions, the Auto Client Reconnect feature uses the cookie on the client device to disconnect an active session before attempting to reconnect.

Sometimes automatic reconnection can result in a new ICA session instead of a reconnected session. A new session can be created if:

- The cookie on the client containing the key to the session ID and credentials expires. When the session started originally this cookie was sent to the client. This cookie persists on the client for several minutes after a connection breaks.
- The cookie containing the key is not used because the user must provide credentials. When Require user authentication is selected in the Management Console, a dialog box requesting credentials is displayed to a user during automatic reconnection.

The following types of disconnections do not result in reconnection to sessions:

- Users disconnect ICA sessions by exiting applications without logging off. Clients do not make automatic reconnection attempts in this case.
- Disconnected sessions are anonymous. Clients use automatic reconnection to establish network connections but new sessions are started.

Security in Automatic Reconnection

Automatic reconnection incorporates an authentication mechanism based on encrypted user credentials. When a user initially logs on to a server to use an application, MetaFrame XP encrypts and stores the user credentials in memory, creates a cookie containing the encryption key, and sends the cookie to the ICA Client. The client submits the key to the server for reconnection. The server decrypts the credentials and submits them to Windows logon for authentication.

When cookies expire users must resubmit credentials. Cookies are not used if you select Require user authentication. Selecting this option displays a dialog box to users requesting credentials when the ICA Client is attempting to automatically reconnect. Use the Management Console to configure Require user authentication.
For maximum protection of users’ credentials and ICA sessions, use SSL encryption for all communication between ICA Clients and MetaFrame XP servers.

Configuring Reconnection Settings

You can do the following to configure automatic reconnection:

- Require user authentication upon auto-reconnection. The requirement can be set at the server farm level or on individual MetaFrame XP servers.
- Enable or disable logging of reconnection events for the server farm or individual servers.
- Enable or disable auto reconnect functionality at the ICA Client using an ICA file or Appsrv.ini.

By default, auto reconnection is enabled and user authentication is not required.

You can use the Management Console or the Acrcfg command to require user authentication for automatic reconnection and reconnection event logging. Reconnection event logging is disabled by default. For more information about the Acrcfg command, see "MetaFrame XP Commands" on page 311.

You can disable auto reconnect functionality on the ICA Win32 Client by setting TransportReconnectEnabled=Off in the [WFClient] section of the client’s Appsrv.ini file. For more information about client configuration using Appsrv.ini, see the ICA Win32 Client Administrator’s Guide.

Settings for ICA connections also affect the auto reconnect feature.

Setting Up ICA Connections for Auto Client Reconnect

By default, automatic reconnection is enabled in a server farm. However, if a server’s ICA TCP connection is configured to reset sessions with a broken communication link, automatic reconnection does not occur. The auto reconnect feature works only if the server disconnects sessions when there is a broken or timed-out connection.

In this context, the ICA TCP connection refers to a MetaFrame XP server’s virtual port (rather than an actual network connection) that is used for ICA sessions on TCP/IP networks.

By default, the ICA TCP connection on a MetaFrame XP server is set to disconnect sessions with broken or timed-out connections. Disconnected sessions remain intact in system memory and are available for reconnection by the ICA Client.
Chapter 11 Managing Users and ICA Sessions

The ICA connection can be configured to *reset*, or log off, sessions with broken or timed-out connections. When a session is reset, attempting to reconnect initiates a new ICA session; rather than restoring a user to the same place in the application in use, the application is restarted.

If MetaFrame XP servers are configured to reset sessions, the automatic reconnection sequence creates a new ICA session on the initial host. This process requires users to enter their credentials to log on to the server.

- **To configure the ICA TCP connection for auto reconnect**
  1. Run Citrix Connection Configuration (choose Start > Programs > Citrix > MetaFrame XP > Citrix Connection Configuration).
  2. In the Citrix Connection Configuration window, double-click the ica-tcp connection. The Edit Connection dialog box appears.
  3. In the Edit Connection dialog box, click Advanced.
  4. In the Advanced Connection Settings dialog box near the bottom, the first pop-up menu sets the behavior for a broken or timed-out connection.

- If Inherit User Config is selected, you cannot change the setting because the connection inherits the setting from each user’s profile.
- When Inherit User Config is not selected, you can select one of the following options to configure the ICA TCP connection:
  - **Disconnect.** The server places broken connections in the disconnected state. The ICA Client can reconnect automatically without any action by users.
  - **Reset.** The server resets broken connections. Automatic reconnection creates a new ICA session and requires users to reenter credentials.

Be sure to select **Disconnect** to set up the ICA TCP connection to work with the auto client reconnection feature.
5. Click **OK** to close the dialog box and the previous dialog box. Then, choose **Connection > Exit** to close Citrix Connection Configuration.

- **To configure an ICA connection for individual users**

  In the **Advanced Connection Settings** dialog box, if **Inherit User Config** is selected for the setting labeled **On a broken or timed-out connection**, the connection inherits the setting from each user’s profile. To view or change the setting for broken or timed-out connections, do the following to display the properties for each user.

  On servers running Windows 2000, use **Computer Management** to configure user profiles.

  1. Double-click a user to open the **Properties** dialog box.

  2. On the **Sessions** tab, check the setting under **When a session limit is reached or a connection is broken**.

  3. Select **Disconnect from session** to allow automatic reconnection.

```plaintext
<table>
<thead>
<tr>
<th>General</th>
<th>Member Of</th>
<th>Profile</th>
<th>Environment</th>
<th>Sessions</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Use this tab to set Terminal Services timeout and reconnection settings</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>End a disconnected session:                 Never</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Active session limit:                       Never</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Idle session limit:                         Never</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>When a session limit is reached or connection is broken:</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Disconnect from session</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>- End session</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
```

**Logging Reconnection Events**

To enable or disable log entries for automatic reconnection events, use **ICA Settings** in the **Properties** pages for the server farm or individual MetaFrame XP servers.

Logging is disabled by default. When logging is enabled, the server’s System log captures information about successful and failed automatic reconnection events to help with diagnosis of network problems.
Automatic reconnection can fail if the ICA Client submits incorrect authentication information (which might occur during an attack) or the server determines that too much time has elapsed since it detected the broken connection.

Each server stores information about reconnection events in its own System log. The server farm does not provide a combined log of reconnection events for all servers.

Creating and Applying User Policies

You can create user-based policies to apply select MetaFrame XP settings to specific Windows domain users or user groups.

By creating and applying user-based policies you can:

- Allow users to shadow other users’ ICA sessions
- Control access to drives, ports, and printers on client devices
- Set a required encryption level for ICA sessions
- Turn off the Auto Client Update feature for specific users

Because policies are applied to users or user groups when they log on to the MetaFrame XP farm, policies follow users no matter which client devices they use. A policy’s rules remain in effect for the length of the user’s ICA session. In general, user policies override similar MetaFrame XP settings configured for the entire server farm, for specific servers, or on the ICA Client. However, the highest encryption setting and the most restrictive shadowing setting always override other settings.

With user policies, you can tailor MetaFrame XP to meet users’ needs based on their job functions, geographic locations, or connection types (LAN, WAN, or dial-up). For example, for security reasons you may need to place restrictions on user groups who regularly work with highly sensitive data. You can create a policy that requires a high level of encryption for ICA sessions and prevents users from saving the sensitive files on their local client drives.

However, if some of the people in the user group do need access to their local drives, you can create another policy for only those users. You then rank or prioritize the two policies to control which one should take precedence.

Policy rules have three states: enabled, disabled, or not configured. By default, all rules are not configured. All unconfigured rules are ignored when users log on to the MetaFrame XP server, so the rule comes into play only when the state is enabled or disabled.

The basic steps for effectively creating and using policies are as follows. These steps are explained in more detail below.
1. Decide the criteria on which to base your MetaFrame XP policies.
   You may want to create policies for users and user groups based on job function, connection type, or geographic location, or you may want to use the same criteria that you use for your Windows Active Directory group policies.

2. Create the policy. Creating a policy involves the following steps:
   - Naming the policy
   - Assigning the policy to users
   - Setting the policy’s rules

3. Prioritize or rank your policies
   When you create policies for entire user groups, you may find that some members of the group require exceptions to some policy rules. To more effectively manage your policies, you can create new policies for only those users who need exception to a policy’s rules, and then rank the policy for those individual users higher than the policy for the entire group.

You can use the Search tool in the Management Console to find which policies are applied to which users, and to determine the effective rule settings when more than one policy is applied to the same user.

To use the Search tool, open the Management Console and click the **Search** button. See the console’s online Help for more information about Search.

### To create a new user policy

1. In the Management Console for MetaFrame XP, right-click the Policies node in the left pane and choose **Create Policy** or click the **Create Policy** button on the console toolbar.

2. Enter the name of the policy in the **New Policy** dialog box and then click **OK**. Examples of policy names are “Accounting Department” or “Remote Users.” The policy name is displayed in the right pane of the console.

3. You can add a description of the policy by right-clicking the policy and selecting **Edit Description**.

4. Apply the policy to users or user groups by right-clicking the policy name and choosing **Assign Users**. Double-click a domain name to display user groups. Select **Show users** to display individual user accounts.
5. Select the user group and/or users to whom you want to assign the policy and then click Add.

By default, the policy is allowed for any users or user groups you add to the configured accounts list. If there are members of the user group you do not want assigned to this policy, you can add the individual members of the group and then select Deny to prevent the policy from being applied to them.

Click OK when you are done adding users.

6. You set the policy’s rules on the policy’s property sheet. Double-click the policy to open its property sheet. Some policy rules are organized into folders. Expand the folders to view the rules you can apply.

7. When setting policy rules, determine which settings you want to apply. Click Enabled to apply the rule to the assigned users or user groups. For more information about policy rules, select the rule in question and then click Help.

8. Click OK when you are done.

Prioritizing Policies

After you create basic policies using your primary criteria, you may find that you need to create additional policies for individual users who require exceptions to some policy rules.

In the following procedure, the interwoven example assumes that you created a policy for your “Accounting” user group. One of the rules enabled in this policy prevents the user group from saving data to their local drives. However, two users who are members of the Accounting group travel to remote offices to perform audits and need to save data to their local drives.

The steps below describe creating a new policy for Accounting group members Carol and Martin that will allow them access to their local drives while allowing the other policy rules to work the same way for them as for all other members of the Accounting group.

To create exceptions and prioritize policies

1. Determine which users need additional policies to create exceptions.

   The policy named “Accounting Profile” that is assigned to the Accounting group includes a rule that prevents access to local drives. Carol and Martin, members of the Accounting group, need access to their local drives.

2. Determine which rule or rules you do not want to apply to these users.

   You want most of the rules in this policy to apply at all times to all users, with the exception of the rule that prevents access to local drives.
3. Create a new policy. See “To create a new user policy” on page 282 for more information. You may want to name this policy “Accounting Profile - local drive access.”

4. Edit the description of the policy by right-clicking the policy and selecting Edit Description. You can use policy descriptions to help you keep track of your policies.

5. Open the policy’s property sheet and locate the rule you do not want to apply to Carol and Martin. Set the rule’s state to Disabled.

6. Assign users Carol and Martin to the policy by right-clicking the policy name and choosing Assign Users. Select the Show Users option to display individual user accounts.

7. Click OK when you are done adding users.

8. Rank the “Accounting Profile - local drive access” policy higher than the “Accounting Profile” policy. By default, new policies are given the lowest rank.

Right-click the “Accounting Profile - local drive access” policy and select Priority > Increase Priority until this policy’s priority number is lower than the “Accounting Profile” policy. A policy with a priority number of 1 has the highest priority.

## Shadowing ICA Sessions

You can monitor the actions of users in ICA sessions by shadowing their sessions. A shadowed session is displayed in the session of the shadower, the user who establishes shadowing.

Shadowing an ICA session provides a powerful tool for you to assist and monitor users. Shadowing is a useful option for your Help desk staff, who can use it to aid users who have trouble using an application. Help desk personnel can view a user’s actions to troubleshoot problems and can demonstrate correct procedures. You can also use shadowing for remote diagnosis and as a teaching tool.

You can create a user policy to enable user-to-user shadowing. When you create a policy allowing user-to-user shadowing, users can shadow other users without requiring administrator rights. Multiple users from different locations can view presentations and training sessions, allowing one-to-many, many-to-one, and many-to-many online collaboration. See “Configuring User-to-User Shadowing” on page 286 for more information about user-to-user shadowing.

A shadower can remotely control a shadowed session through the shadower’s mouse and keyboard, if this action was not prohibited by options selected when MetaFrame XP was installed on the server.
Important  If shadowing restrictions are selected during MetaFrame XP installation, the restrictions cannot be changed later. For more information, see “Configuring Session Shadowing” on page 123.

By default, the user who will be shadowed is asked to accept or deny the request to shadow the ICA session.

You can shadow multiple sessions using the Management Console or the Shadow Taskbar.

**Shadowing from Citrix Management Console**

When you use the Management Console for shadowing, you must start each shadowing session individually; if you select multiple sessions to shadow, the Shadow command and button are not available. To start shadowing multiple sessions at once, use the Shadow Taskbar.

To use the Management Console for shadowing, you must have the ICA Client installed on the system with the console. The ICA Client is installed by default when you install MetaFrame XP on a server, but the client is not installed when you install the Management Console separately on a workstation. You can use the Citrix MetaFrame XP Components CD-ROM to install the ICA Client on a workstation.

1. On the Users or Sessions tab in the right pane of the console, right-click the user or session that you want to shadow.
2. Choose Shadow from the pop-up context menu.

To begin shadowing, you can also select a user or session listing and click the Shadow button on the console toolbar.

**Using the Shadow Taskbar**

To launch the Shadow Taskbar, choose Start > Programs > Citrix > MetaFrame XP > Shadow Taskbar. The Shadow Taskbar appears as a toolbar at the top of the console display.

Tip  You can click the Shadow Taskbar button on the ICA Administrator toolbar to launch the Shadow Taskbar.

When the Shadow Taskbar is running and no sessions are being shadowed, the Shadow button appears alone on the Taskbar. Click the Shadow button and the Shadow Session dialog box appears.
Use the **Shadow Session** dialog box to select the sessions you want to shadow. You can select sessions based on the server, the application, or the users who are associated with the sessions. You can select multiple sessions in the dialog box to begin shadowing several sessions at once. Click **OK** to begin shadowing the selected sessions.

For more information about shadowing with the Shadow Taskbar, press F1 to view online help when the Shadow Taskbar is running.

### Configuring User-to-User Shadowing

You can monitor the actions of users in ICA sessions by shadowing their sessions. A shadowed session is displayed in the session of the *shadower*, the user who establishes shadowing.

With user-to-user shadowing, you can allow users to shadow other users, without requiring them to be members of the MetaFrame XP Administrators group. Multiple users from different locations can view presentations and training sessions, allowing one-to-many, many-to-one, and many-to-many online collaboration.

With user-to-user shadowing, you can enable Help Desk personnel to shadow users’ ICA sessions or allow your sales department to hold an online meeting to review sales leads.

The basic steps for configuring user-to-user shadowing are as follows. These steps are explained in more detail later in this section.

1. Create a user policy that identifies the users who can shadow other users’ sessions
2. Assign the policy to the users to be shadowed
3. Publish the Citrix Shadow Taskbar and assign it to the users who will shadow
4. Instruct these users how to initiate shadowing from their client devices

**Note** You are prompted to configure shadowing settings during MetaFrame XP Setup. If you elected to prohibit shadowing during Setup, you cannot enable shadowing with user policies. You can also disable shadowing for a particular connection type using the Citrix Connection Configuration utility. If you disable shadowing in Citrix Connection Configuration, you cannot enable shadowing with user policies.

### Creating User Policies for User-to-User Shadowing

You configure user-to-user shadowing by creating user policies that define users who can shadow. You then assign the policies to the users you want to be shadowed.
Important You can create and apply a policy that allows Novell Directory Services (NDS) users to be shadowed. However, you cannot configure NDS users to have shadowing permissions.

In the following procedure, the interwoven example assumes that you want to create a policy for your “Sales” user group that allows them to shadow the department manager, AnthonyR. The sales department uses the user-to-user shadowing feature for online collaboration on sales leads.

To create a user policy for user-to-user shadowing

2. Open the Sales Group Shadowing policy’s property sheet by double-clicking the policy name.
3. Open the Shadowing folder in the left pane. Select the rule named Configure User Shadowing.
4. Set the rule’s state to enabled by clicking Rule Enabled.
5. Click Allow shadowing to enable shadowing.
   Because the sales manager may work with sensitive data, select the option Prohibit being shadowed without notification.
   If the sales manager does not want other users to be able to take control of his mouse and keyboard, select the option Prohibit remote input when being shadowed.
6. Select the rule named Assign Shadowing Permissions in the left pane of the property sheet.
7. Set the rule’s state to enabled by clicking Rule Enabled.
8. Click Configure to select the users who will shadow the sales manager.
   To allow the members of the sales department to shadow the sales manager, select the Sales user group and then click Add. The user group is listed in the Configured Accounts list.
   Click OK when you are done adding users.
9. The users and user groups you added to the Configured Accounts list are listed in the right pane of the policy’s property sheet. By default, the shadowing permission for each user or user group is set to Allow. You can deny shadowing permissions by clicking Deny.
10. Click **OK** at the bottom of the policy’s property sheet when you are done configuring the shadowing rules.

After you create the policy and configure the rules, you must assign the policy to the users who you want to be shadowed.

- **To assign the shadowing policy to users**
  1. Right-click the Sales Group Shadowing policy and select **Assign Users**.
  2. Select the users you want to be shadowed. To allow the sales manager, AnthonyR, to be shadowed, select the domain of which he is a member. Click **Show Users** to display the individual user accounts in the selected domain.
  3. Select the user AnthonyR and then click **Add**. AnthonyR’s user account is displayed in the Configured Account list.
  4. Click **OK** when you are done adding users.

---

**Important** The list of users permitted to shadow is exclusive for each user to whom a policy is assigned. For example, if you create a policy that permits user MichelleF to shadow user LorenaB, this policy allows only MichelleF to shadow LorenaB, unless you add more users to the list of users who can shadow in the same policy’s property sheet.

To allow users to shadow other users’ ICA sessions, you can publish the Shadow Taskbar utility to the users you want to be able to shadow. When users open this published application, the Shadow Taskbar appears at the top of users’ screens.

For more information about using the Shadow Taskbar to shadow ICA sessions, see “Using the Shadow Taskbar” on page 285 and the Taskbar’s online help.

---

**Monitoring Performance of Sessions and Servers**

Performance monitoring counters for ICA data are installed with MetaFrame XP and can be accessed from Performance Monitor, which ships with the Windows operating system.

By using Performance Monitor, you can monitor the following ICA-specific counters:

- Bandwidth and compression counters for ICA sessions and MetaFrame XP servers
- Bandwidth counters for individual virtual channels within an ICA session
- Latency counters for ICA sessions
The entire ICA counter list is exposed only on a MetaFrame XPe server. On a MetaFrame XPa or MetaFrame XPs server, only latency-related counters are available.

Performance monitoring provides valuable information about utilization of network bandwidth and helps determine if a bottleneck exists.

To access ICA performance counters

1. Select Start > Programs > Administrative Tools > Performance.
2. Select System Monitor in the Tree view.
3. Click Add.
4. In the Add Counters dialog box, click the Performance object drop-down list and select ICA Session.
The ICA performance counters are listed under **Select counters from list**.

5. Select **All Counters** to enable all available ICA counters or select **Select counters from list** and then highlight the individual counters you need.

6. Select **All Instances** to enable all instances of the selected ICA counters or select **Select instances from list** and highlight only the instances you need.

In Performance Monitor, the instance list contains all active ICA sessions, which includes any session (shadower) that is shadowing an active ICA session (shadowee). An active session is one that has been successfully logged on to and is in use; a shadowing session is one that initiated shadowing of another ICA session.

**Note** In a shadowing session, although you are able to select ICA counters to monitor, you will see no performance data for that session until shadowing is terminated.

7. Click **Add** and then click **Close**.

You can now use Performance Monitor to view and analyze performance data for the ICA counters you added. For more information about using Performance Monitor, see your Windows documentation.
Users can print documents easily when they run applications on MetaFrame XP servers. For most users, printing when they use applications in ICA sessions is no different from printing from applications that run on their own computers.

This chapter describes MetaFrame XP features for making printers available to users and managing printers in MetaFrame XP server farms.

To find step-by-step instructions for using the features that are described in this chapter, use the online help feature in the Management Console for MetaFrame XP.

For more information about printing configuration and options for ICA Clients, see the *ICA Client Administrator's Guide* for the ICA Clients you plan to deploy.

**Overview of Printing with MetaFrame XP**

When users run applications that are published on MetaFrame XP servers, they can print to the following types of printers:

- Printers that are connected to ports on the users’ client devices on Windows, WinCE, DOS, and Mac OS platforms
- Virtual printers created for tasks such as printing from a PostScript driver to a file on a Windows client device
- Shared printers that are connected to print servers on a Windows network
- Printers that are connected directly to MetaFrame XP servers

The printers that ICA Clients can use can be categorized by connection types. You can set up three general types of printer connections in a MetaFrame XP server farm: client connections, network connections, and local connections. Therefore, this chapter refers to printers in a server farm as client printers, network printers, and local printers, depending on the type of connection they have in the farm.

**Client printers.** The definition of a *client printer* depends on the ICA Client platform.
On DOS-based and WinCE client devices, a client printer is physically connected by a cable to a port on the client device. A PC or PostScript printer connected to a serial port on a Mac OS system is also considered a client printer.

On 32-bit Windows platforms (Windows 9x, Windows NT, and Windows 2000), any printer that is set up in Windows (these printers appear in the Printers folder on the client device) is a client printer. Locally connected printers, printers that are connected on a network, and virtual printers are all client printers.

**Note** Some virtual printers, such as a fax/modem device that is set up in the Printers folder, might not be available as a client printer in ICA sessions.

When a user shares a client printer through Windows printer sharing, the printer appears as a network printer to other users.

**Network printers.** Printers that are connected to print servers and shared on a Windows network are referred to as network printers. In Windows network environments, users can set up a network printer on their computers if they have permission to connect to the print server. When a network printer is set up for use on an individual Windows computer, the printer is a client printer on the client device.

**Local printers.** Printers that are connected directly to MetaFrame XP servers are local printers within a particular server farm. This definition includes a printer that is connected to the MetaFrame XP server that hosts a user’s ICA session, as well as printers that are connected to other MetaFrame XP servers in the same server farm.

If a printer is connected to a MetaFrame XP server outside of a server farm (either the server is not a member of a server farm or is a member of a different server farm), the server farm considers the printer a network printer, not a local printer.

**Client Printing in ICA Sessions**

The following list summarizes the types of printers that can be available for an ICA Client, based on the printer definitions above. Depending on the user’s platform and the printers that exist in the farm, a user who connects to a MetaFrame XP server and runs a published application or desktop in an ICA session can print to the following:

- The user’s own client printers
- Network printers that are set up for the farm
- Local printers on the MetaFrame XP server that hosts the user’s ICA session
- Local printers on other MetaFrame XP servers that are set up for use in the farm
It is important to note that printer availability can vary with the client device. For specific information about printing capabilities, see the *ICA Client Administrator’s Guide* for each ICA Client you plan to deploy.

**Printing Configuration Scenarios**

The previous section describes printers that can be used by ICA Clients. Some printers can be used without being set up specifically for use in a MetaFrame XP server farm. For example, you can make client printers available for ICA Client users on Windows devices without configuring printers on each client device.

This section describes when and how you need to set up and configure printers for ICA Clients. It gives an overview of the configuration features available in MetaFrame XP through the Management Console.

The steps required to set up printers for use by your ICA Client users depends on the configuration of the clients, the type of printers you use and their connections, and the configuration of your application servers.

For example, two scenarios for printing appear below. For more information about the printer management setup mentioned in these scenarios, see the feature descriptions later in this chapter.

**Scenario 1: Printers Installed on Windows Clients**

Users run Windows 2000 or higher on their client devices. Printers are already set up for all users on their client devices (so they can print from applications that they run locally). Some users have PC printers connected directly to their computers, while others print to shared network printers.

In this type of environment, you can set up printers in the server farm by simply installing printer drivers on a MetaFrame XP server and using the replication feature in the Management Console to distribute the drivers to all the servers in the farm.

- The printers that users normally print to are available automatically when they connect to MetaFrame XP servers, because MetaFrame XP creates each user’s client printers for use during ICA sessions.

- Because printer drivers installed on client devices running Windows 2000 or higher are the same drivers you install on Windows Servers, you do not need to set up printer driver mapping. Mapping is necessary when the printer drivers you install for Windows 9x client computers and Windows servers have different names.
When users print from applications running on MetaFrame XP servers, the installed client printers appear in Windows in the following form: `#clientname/printername`. The `clientname` is the name of the client device and `printername` is the name for the installed client printer.

**Scenario 2: Network Printers in a Mixed Environment**

In a typical mixed computing environment, users run ICA Clients on a variety of operating systems. Some, but not all users, might have printers connected to their client devices. Shared printers on network print servers might be available to all users, but they might not be set up because users are untrained or because administrators do not want to set up individual clients in a new network deployment or an application service provider environment.

In these situations, you can make printers available easily through MetaFrame XP. MetaFrame XP can automatically create client printers for the client devices that have printers installed. For the entire user base, you can set up network printers to be used by ICA Client users on all client platforms.

- You make printers that are already installed on client computers available in ICA sessions by installing printer drivers on a MetaFrame XP server and using the replication feature in the Management Console to distribute the drivers to all servers in the farm. MetaFrame XP automatically creates these client printers when users connect to servers in the farm.

- When some users have Windows 9x client devices, you map client printer drivers to the drivers you install on MetaFrame XP servers. This is necessary when driver names for the same printer are different on client devices running Windows 9x and on the Windows 2000 servers. Driver mapping is not necessary for client devices running Windows 2000 or higher, because they use the same printer drivers as Windows 2000 servers.

- You import network print servers into the MetaFrame XP server farm to make the shared printers available to all users when they connect to servers in the farm.

- If some client printer drivers are not compatible with the MetaFrame XP server platforms in the farm, use the Driver Compatibility feature to prevent incompatible printer drivers from causing server errors.

- When users print from applications running on MetaFrame XP servers, the installed client printers appear in Windows in the following form: `#clientname/printername`. The `clientname` is the name of the client device and `printername` is the name for the installed client printing device.

- When users print to the network printers in the server farm, they see the original assigned network printer names in Windows dialog boxes.
Printer Management Features

The Management Console for MetaFrame XP provides access to all MetaFrame XP printer management features. You use the Management Console to monitor and configure printers for users in a server farm.

To make changes to printer configurations, you must be a MetaFrame XP administrator with the right to manage the Printer Management node.

For information about using the Management Console, see “To use the Management Console” on page 177.

You can use MetaFrame XP printer management features from several views in the Management Console. The first parts of this section describe the console views you can use for managing printers for users, and the information you can monitor from the tabs in the console’s right pane.

After you launch the console and log on to a MetaFrame XP server in the server farm, the left pane in the console displays the tree view of the server farm management nodes. When you select an item in the tree, the right pane displays one or more tabs.

Select the Printer Management node or the Servers node or the objects under these nodes to use the primary printer management features in the console.

```
Printer Management
  Drivers
  Printers
  Servers
```

Using the Printer Management Node

When you select Printer Management in the console tree, the right pane displays tabs labeled Contents, Bandwidth, and Network Print Servers (the default tab).

When you expand the Printer Management node, the left pane displays objects labeled Printers and Drivers in the tree.

Contents Tab

When you select Printer Management, the Contents tab displays objects labeled Drivers and Printers. The same objects appear in the tree under Printer Management when you expand the node.
Double-clicking an object on the Contents tab is the same as selecting the object in the tree. Either action changes the right pane to display information about the object you select, and puts commands related to the object in the Actions > Printer Management submenu and on the console toolbar.

**Network Print Servers Tab**

Use the Network Print Servers tab to view the names of network print servers whose printers can be configured in the server farm. When you create a new MetaFrame XP server farm, the tab lists nothing until you import one or more network print servers.

After you import print servers, the Network Print Servers tab displays the name of each print server and the date and time when the console last updated the print server information. The tab uses the time zone of the machine to which the console is connected for the date and time display.

**Importing print servers.** Use the Network Print Servers tab when you want to import a network print server to make its printers available to the users of the server farm. When you select the tab, you can choose Import Network Print Server from the toolbar or the Actions menu. The command and toolbar button are not available when other tabs are selected.

**Tip** Importing a network print server lets users in the server farm use a printer that is not connected to their client device. Client printers are automatically made available to users in their ICA sessions.

**Updating server information.** If you add printers to or remove them from a network print server, update the print server information to be sure that the console displays the available printers on the Printers tab. To do this, select a print server and use the Update Network Print Server command from the right-click menu, the toolbar, or the Actions menu. You must take this action because updating print server information does not take place automatically.

**Removing print servers.** Removing a print server removes all of its printers from the farm. This is the opposite of importing a network print server. If you remove printers, ICA Client users cannot print to them. If you want to do this, select the print server to remove, and then choose Discard Network Print Server from the right-click menu, the console toolbar, or the Actions menu. After you confirm the command, the printer server no longer appears on the Network Print Server tab and its printers do not appear on the Printers tab.
Bandwidth Tab

When you select Printer Management in the console tree, the Bandwidth tab displays the print stream bandwidth setting for each server in the farm. Use this tab to set or remove print stream bandwidth limits on MetaFrame XP servers and copy settings from one server to others. Limiting printing bandwidth can improve application performance for clients when printing and application data must compete for limited bandwidth.

When you select a server in the list on the Bandwidth tab, you use the Edit command to change its bandwidth setting, or use the Copy command to copy its bandwidth setting to one or more servers in the farm. You can use these commands from the right-click menu, the console toolbar, or the Actions menu.

When you select the Servers node in the tree, the Printer Bandwidth tab provides the same display and features as the Bandwidth tab when you select Printer Management.

You can use Printer Bandwidth in the left pane of a server’s Properties page to edit the server’s print stream bandwidth setting.

For more information about limiting the bandwidth of print data streams, see “Limiting Printing Bandwidth in ICA Sessions” on page 309.

Drivers Tab

When you select Drivers in the tree, the Drivers tab in the right pane displays information about printer drivers installed on MetaFrame XP servers. Use this tab to make sure printer drivers are installed and available as necessary on servers in the farm, and to copy them to other servers.

The tab lists any driver installed on a MetaFrame XP server in the farm. The tab does not list drivers that are installed on network print servers (non-MetaFrame XP servers). You must manually install drivers for all printers that ICA Client users need for printing from ICA sessions, including client printers and network printers.

The driver information includes each driver’s name and operating system platform. You select a specific server from the Server drop-down menu to display the drivers installed on one server, or select (Any) to display all drivers on all servers in the farm.

Use the Drivers tab to copy printer drivers to other servers in a server farm. If printer drivers are not already installed, copy the drivers to each server where ICA Client users log on and need access to the driver for printing to client printers or network printers.

To copy a driver, select the driver and then use the Replicate Drivers command from the console toolbar, the right-click menu, or the Actions menu.
Two tabs in the Management Console show printer driver information. To display the drivers installed on a MetaFrame XP server, you can select the server from the Server menu on the Drivers tab, or select the server in the console tree and look at the Printer Drivers tab. You can use either tab to copy printer drivers to other servers in a farm.

Printers Tab

When you select Printers in the Management Console tree, the Printers tab in the right pane lists all printers that you can configure in the server farm. The list includes the following printers:

- Local shared printers that you install and connect directly to MetaFrame XP servers in the farm
- Network printers that are installed and connected to network print servers when you import the print servers into the farm

The printer list shows the printer name, print server name, driver name, and MetaFrame XP operating system platform for each local printer. For network printers, the list shows only the printer name and print server name.

You can select a local printer on the Printers tab and use the console to copy the drivers and settings for the printer to other servers. You cannot copy a driver of a network printer from this tab. (Use the Drivers tab to copy drivers from a MetaFrame XP server to other servers.)

Select a printer and use the Auto-Creation command to assign users to the printer. Auto creation makes a printer available in ICA sessions for the users you specify. If you want to allocate other printers to the same users, select a printer and copy its auto creation settings from this tab.

Using the Servers Node

When you select Servers in the Management Console tree, multiple tabs appear in the right pane. The tab that relates to printer management is the Printer Bandwidth tab. This tab displays the same information as the Bandwidth tab that appears when you select Printer Management in the console tree. See “Bandwidth Tab,” above.
Printers Tab

When you select a MetaFrame XP server in the console tree under the Servers node or on the Contents tab, the Printers tab displays information about a server’s local printers. The tab displays information about the printers that are connected directly to the server, if you select the Shared option when you install the printers. Printers that you do not share do not appear on the tab.

This tab is similar to the Printers tab that appears when you select Printers in the console tree. However, when you select one server, the Printers tab displays only the server’s local printer information, not information about network printers in the farm.

You can select a local printer on the Printers tab and use the console to replicate the drivers and settings for the printer to other servers. You can also assign users to the printer to make it available as an auto created printer in the users’ ICA sessions. If you want to assign the same users to another printer, select the printer and copy its auto creation settings from this tab.

Printer Drivers Tab

When you select a MetaFrame XP server in the console tree (under the Servers node), the Printer Drivers tab lists printer drivers that are installed on the server. Select a driver name in the list to display the names of all the servers that have the driver installed. Use the Replicate Drivers command to copy the driver to other servers in the farm. You need to copy printer drivers to each server where ICA Client users log on and need access to the driver for printing to client printers or network printers.

The Printer Drivers tab displays the same information as the Drivers tab displays when you select Drivers in the console tree.

Setting Up Network Printers for ICA Client Users

To make network printers available to ICA Client users, you import network print servers into the MetaFrame XP server farm. Doing this makes all printers that are connected to the print server available to the ICA Client users that you specify. After you install required printer drivers, ICA Client users can print to these printers in their ICA sessions. You use the Management Console to perform these procedures.
To make network printers available to ICA users

The following steps outline the procedure for setting up network printers for ICA Client users. For detailed instructions, use the Help menu or click Help on the toolbar and dialog boxes in the Management Console for MetaFrame XP.

1. Import network printers from a network print server into the farm. Select Printer Management in the Management Console, select the Network Print Servers tab, and choose Import Network Print Server. Specify the network print server to import.

   When the operation finishes, the print server appears on the Network Print Servers tab in the console.

2. Install the printer drivers for your network printers on a MetaFrame XP server in the server farm. Use the Replicate Drivers command to distribute the drivers to all the MetaFrame XP servers in the farm.

3. Allocate network printers to users. Select a printer on the Printers tab and choose Auto-Creation. Specify a domain and select the groups and users who need to use the printer.

   When a specified user logs on to a MetaFrame XP server in the farm, the printer becomes available in the user’s ICA session as if the printer is installed on the user’s client device.

4. To set up additional printers for ICA Client users, select the printer you allocated to users. Choose Copy Auto Creation Settings to copy the printer’s user list to other printers in the farm.

   Tip Because you set up printers for auto creation by user account, the users can log on to applications from different client devices and use the same network printers. (Because client printers are connected directly, they are available only from the client devices where they are installed.)

5. If necessary, map client printer drivers to server drivers if the driver names are different on each platform. For details, see “Mapping Printer Drivers” on page 302.

Installing and Replicating Printer Drivers

To install printer drivers on a MetaFrame XP server, you use the standard Windows printer installation methods. The Add Printer wizard asks for information about a printer and copies the necessary driver files. You might need to insert a Windows installation CD-ROM or media from the printer manufacturer so the wizard can copy the files.
When you use the wizard to install drivers on a MetaFrame XP server, the actual printer is not attached to the server. Select the **Local** option and select any local printer port that does not have an actual printing device connected; you can add multiple printers to one port.

**Tip**  In server farms where it is practical do to so, install all driver files on one server.

After you install drivers, you can use the driver replication feature in the Management Console to copy the driver files and registry settings to other servers in the server farm. Use the replication feature to save time when you install printer drivers, and to ensure that all drivers are available on all servers where ICA Clients need them, so that the ICA Client users can print to the client and network printers in the farm.

**Important**  Because printer drivers are platform-specific, do not replicate drivers from a MetaFrame XP server to servers on a different platform. When the **Drivers** tab in the console lists drivers from both platforms and you choose **Replicate Drivers**, the console warns you about this because you can select drivers on either platform to replicate.

### Setting Up Automatic Replication of Printer Drivers

You can set up automatic printer driver replication so MetaFrame XP performs replication when you add a server to the farm, or when you restart a server in the farm.

MetaFrame XP maintains one auto-replication list for each platform in the server farm. When you select a printer driver for replication, MetaFrame XP adds the driver to the appropriate auto-replication list. You can add or remove drivers from the auto-replication lists by choosing **Auto-Replication** from the **Drivers** tab in the console.

When you edit the auto-replication list, you can use one server or any server as the source for a particular printer driver. If you specify any server, MetaFrame XP will copy the driver from any server that is available in the farm at the time of auto-replication to a new or restarted server. This setting avoids the possibility that a specific source server for a printer driver might be unavailable when new or restarted servers need to receive a printer driver.

MetaFrame XP cannot replicate drivers from network printers (printers installed on network print servers) because MetaFrame XP does not have guaranteed access to the driver files.
If driver replication fails because of communication errors, the console displays an error message and records the error in the server Event Log for each server where the operation failed.

**Mapping Printer Drivers**

Mapping of printer drivers refers to identifying printer drivers that have different names for the same printer on different Windows platforms. You need to use mapping if drivers you install on MetaFrame XP servers have names different from the drivers used by Windows 9x computers for their client printers.

Printer mappings are listed in a Citrix file, Wtsprnt.Inf. Select Drivers in the Management Console and choose **Mapping** from the **Actions** menu to manage printer driver mapping for a server farm.

In the **Driver Mapping** dialog box, you choose a server platform (because drivers differ on Terminal Server and Windows 2000 servers) and add the names of client printer drivers that correspond to the drivers you install on MetaFrame XP servers in the farm.

---

**Note**  When you designate a printer driver to be incompatible for client printers in the farm (see “Managing Drivers for Client Printers” on page 302), you cannot create a printer driver mapping with the same driver.

---

**Managing Drivers for Client Printers**

Some printer drivers can cause server problems when users print to client printers in the server farm. Because printing to a client printer with a badly behaved driver can cause a fatal system error on a server, you might need to prevent auto creation of client printers that use certain printer drivers.

If a defective driver is replicated throughout a server farm, it is difficult and time consuming to remove it from every server to prevent its use with client printers. However, you can accomplish the same result with the Management Console. Use the printer driver compatibility feature to designate drivers that you want to allow or prohibit for use with client printers.

**Maintaining Driver Compatibility Lists**

MetaFrame XP has a driver compatibility list for each server platform in use in the server farm. To add or remove drivers, or edit the driver names in the compatibility list, select Drivers in the console tree and choose **Compatibility** from the **Actions** menu or the console toolbar.
Use the **Driver Compatibility** dialog box to manage the printer driver compatibility list for each server platform. You can list the printer drivers you allow or the drivers you do not allow to be used in the farm. To add drivers to the list, choose from the menu of all drivers that are installed on servers in the farm.

MetaFrame XP normally sets up (auto creates) client printers for all users who have client printers installed on their client devices. When users log on, MetaFrame XP checks the client printer driver compatibility list before it sets up the client printers. If a printer driver is on the list of drivers that are not allowed, MetaFrame XP does not set up the printer. When the compatibility list prevents setup of a client printer, MetaFrame XP sends messages to client users and writes a message in the server’s event log.

### Configuring Auto Creation of Client Printers

This section explains how to configure auto creation of client printers for various client device platforms.

#### Auto Creation for DOS and WinCE Clients

MetaFrame XP provides auto creation of client printers (printers that are locally connected to client devices) for DOS and WinCE Clients. Auto creation makes these printers available for the client user for printing from the applications they run in ICA sessions.

Auto created client printers appear in the form `clientname#LPTx`. The machine name of the client device replaces `clientname` and the printer port number replaces `x`.

Right-click **Printers** under Printer Management in the Management Console to monitor and configure printer auto creation for DOS and WinCE Clients.

MetaFrame XP can make the client printers available if you set up auto creation for these ICA Clients from the console. MetaFrame 1.8 can enable auto creation of client printers only if users run the Client Printer utility in an ICA session on the client device.

MetaFrame XP servers send data to the client device to make the client printer available in ICA sessions. You can view the status of DOS and WinCE Client printers in the **Client Printers** dialog box from the console. In the dialog box, the word `<downloaded>` appears in the list when information for client printer setup is sent from the server to the client device.

Use the **Client Printers** dialog box to add, remove, reset, edit, and delete the configuration for DOS and WinCE client printers.
These client printers are available to the individual client users only. A client printer appears in applications running on the server only during the client user’s ICA session.

**Auto Creation for Other Clients**

You configure auto creation settings differently for client printers that are not on DOS and WinCE platforms using the Management Console for MetaFrame XP. Select **Printers** in the left pane of **Printer Management Properties** and choose the **Auto-Create Client Printers when user logs on** option to allow client printers to be automatically created when users log on to ICA sessions. This option is selected by default. If you do not select this option, client printers are not automatically created although users can set up connections to client printers manually.

When **Auto-Create Client Printers when user logs on** is selected, you can configure how the printers work using the following options:

- **Update printer properties at each logon.** Select this option to update client printers on the server using settings from printers on the clients. The client printers are updated when users log on. Do not select this option if you want to retain changes to client printers on the server made during ICA sessions.

- **Inherit client printer's setting for keeping printed documents.** Select this option to use the client printer setting **Keep printed documents** on auto created client printers. The setting determines if printed jobs are saved after users log off from ICA sessions. Saving printed jobs can use a lot of space.

- **Delete pending print jobs at logout.** Select this option to delete pending print jobs when a user logs off. Do not select this option if you want users to see print jobs from prior ICA sessions when they log on.

- **Always create client network printers as client printers.** Select this option if you want the client device and not the MetaFrame XP server to process printing requests. When you select this option, communication from MetaFrame XP servers to client devices is faster when they talk across a WAN. Data sent to the client is compressed, so less bandwidth is consumed as the data travels across the WAN. Additionally, if two network printers have the same name, the printer on the same network as the client is used.

You can specify which printers are auto created by selecting one of the following options:

- **Default client printer only.** Select this option to auto create only the default printer on each client device.
Local (non-network) client printers only. Select this option to auto create only the local client printers on a user’s client device. Local client printers are connected directly to the client device through an LPT, COM, USB, or other local port.

All client printers. Select this option to auto create all of the client printers on a user’s client device.

Use connection settings for each server. Select this option to accept the settings specified for the ICA connection in the Citrix Connection Configuration utility. This option is selected by default.

The term connection refers to the virtual ports that are associated with network protocols on MetaFrame XP servers. To change the connection configuration, launch Citrix Connection Configuration (choose Start > Programs > Citrix > MetaFrame XP > Citrix Connection Configuration), double-click the connection in the Citrix Connection Configuration window, and click Client Settings.

Network printers assigned to users can be updated when users log on. To update network printers with the printing preferences assigned to the printer, select Update printer properties at each logon within Auto-Created Network Printers. Do not select this option if you want to retain changes made by users to their network printer settings during ICA sessions.

Auto Creation and Citrix Connection Configuration

Settings that affect the auto creation of client printers appear in Citrix Connection Configuration. An overview of these settings is included here. For more information about these settings, see the online help for Citrix Connection Configuration. For specific information about ICA Client capabilities and settings, see the Citrix ICA Client Administrator’s Guide for each ICA Client platform.

If the Connect Client Printers at Logon option is selected in the connection properties or user profile, client printers are automatically created when users log on to ICA sessions. MetaFrame XP deletes the printers when users log off if the printers do not contain unfinished print jobs. Changes made by users to their Windows printer settings are not maintained. If print jobs are present, MetaFrame XP retains the printer and its associated jobs.

You can preserve printers to maintain custom print settings. If you do not want auto created printers deleted when users log off, configure the client printer using the Properties dialog box in the server’s Printers folder within an ICA session.

The Properties dialog box displays a Comment field that contains the text “Auto Created Client Printer” for automatically created client printers. If you modify or delete this description, MetaFrame XP does not delete the printer when a user logs off from the server. Subsequent logons by the same user employ the printer already defined and do not modify it.
If a user’s connection profiles do not specify **Connect Client Printers at Logon**, the user can connect to a client printer through Windows printer setup. MetaFrame XP does not automatically delete printers that are set up this way when users log off.

**Using MetaFrame XP Universal Printing**

As described previously in this chapter, MetaFrame XP automatically creates client printers when users log on to MetaFrame XP. With auto creation of client printers, users print to their regular printers from applications that are running on MetaFrame XP servers without having to set up their printers each time they log on.

Auto creation of client printers requires drivers for client printers to be available on MetaFrame XP servers. The driver replication feature helps ease printer driver management (see “Managing Drivers for Client Printers” on page 302). However, maintaining drivers for many different printing devices can cause problems.

MetaFrame XP Universal Printing is designed to avoid problems with driver maintenance and other client printing issues in diverse environments.

**Client Printing with the Universal Driver**

The universal printing feature works as follows:

- A single generic printer driver is used on the server to prepare print jobs. This can be the universal driver for the PostScript (PS) language or the PCL5c or PCL4 variations of the Printer Control Language.
- The generic driver creates a print data stream, spools the print job, and redirects the job to the ICA client.
- The client printer renders the print data stream again using a PCL4, PCL5c, or a PS interpreter.
- The client device’s local printer drivers are used to create print images that can be directed to any printer connected and configured on the client device. Print jobs are not restricted to PCL or PostScript compatible printers.

With generic printer drivers you do not need to install and duplicate a potentially large set of native printer drivers throughout the server farm. You may need to deploy a few specific printer drivers for applications that require options not provided by a universal driver.

You can view the properties of a client printer created with a universal print driver to see the options that are available. A tag in the format [UPD:PCL5c] is appended to the name of a printer created using a universal printer driver.
Which universal driver an ICA client can work with depends on the client device’s version and platform. The application server can determine the highest level of universal driver with which the client is compatible. The server uses that universal driver to create a client printer within the ICA session. The server can then use the universal driver to send print jobs to that client printer. The client printer translates the print data streams into print images for specific devices.

By default, the auto creation process uses the native printer driver for a specific printer on the client device to create the client printer. If the correct native printer driver is not available on the application server, the client printer is automatically created using a compatible universal driver. You can use the Management Console for MetaFrame XP to change the default settings. Select Printers or Drivers in the left pane of the Printer Management Properties page to change settings for client printer auto-creation. Click the Printer Drivers tab to view the universal printer drivers installed on the selected server.

Client Compatibility with the Universal Drivers

Only the 32-bit Windows and Macintosh clients at version 7.0 can use PCL5c. PCL5c provides both color and monochrome printing at 600 dots per inch (dpi) resolution.

PCL4 is available for backward compatibility for earlier releases of ICA Clients. PCL4 supports monochrome printing only up to 300 dpi resolution. PS is available for use with version 7.0 of the Unix ICA client. PS is used for PostScript compatible printers and emulators that are available in Unix environments. The PCL5c and PS drivers ship with MetaFrame XP with Feature Release 3.

Benefits of Using the Universal Drivers

With universal printing, you can avoid the following issues:

- Some native printer drivers, especially those that do not use an advanced page description language such as PCL or PostScript, generate very large print files. These files can cause unacceptable delays when print jobs are spooled from the server to the client over a WAN or other slow connection.

- Many printer drivers are not well tested in a terminal server environment. Some drivers cause frequent fatal system errors and spooler faults. Installing many printer drivers for a large user base can destabilize servers.

- Although driver maintenance is more convenient with MetaFrame XP, the effort required to obtain, install, and manage many different printer drivers for a diverse environment can be substantial. Even with careful maintenance, drivers required for printing to every device might not be installed in the server farm. Missing drivers prevent auto creation of client printers for users.
Specifying Printer Drivers for Client Printing

When client printers are automatically created, you can specify whether they use universal drivers available with MetaFrame XP Universal Printing, native printer drivers that must be installed on the server, or both. To configure driver settings, right-click Printer Management in the Management Console tree and choose Properties. Select Drivers in the left pane. Choose from the following options.

**Native drivers only.** Select this option to use native printer drivers when client printers are auto created. If the native driver is not available on the MetaFrame XP server, the client printer cannot be created on the server. This option disables the MetaFrame XP Universal Printing feature.

**Universal driver only.** Select this option to use universal printer drivers for client printers. Universal drivers provide both color and monochrome printing at 600 dots per inch (dpi). Monochrome printing at 300 dpi is supported on some earlier releases of ICA Clients.

**Use universal driver only if native driver is unavailable.** Select this option to use native drivers for client printers, if they are available. If the driver is not available on the server, the client printer is automatically created with the appropriate universal driver. Select this option if you want to provide printing fault tolerance. Printers are automatically created for users even if native drivers for printing devices are not available on or are incompatible with the MetaFrame server’s operating system.

**Both universal and native drivers.** Select this option to create two versions of each client printer: one with a universal driver and the other with the printer’s native driver (if it is installed on the server). Users can print using either printer version. This option is useful if users need to access special printer features unavailable using a universal driver.

Automatically Installing Native Drivers

You can greatly reduce printer administration by configuring native printer drivers to be installed automatically on MetaFrame XP servers when printers are auto created.

A specific client printer can be created on a server only when its native driver is also installed on the server. A standard set of native printer drivers is provided with Windows. MetaFrame XP can automatically install printer drivers from the standard Windows drivers and automatically create both network and client printers.

Third-party drivers that are not provided with the standard Windows drivers must be manually installed on the server before you can configure MetaFrame XP to automatically create the printers that use those drivers. You can also replicate a third-party driver from another server in the farm.
Select **Automatically install native drivers for auto-created client and network printers** if you want native printer drivers to be installed automatically on MetaFrame XP servers when printers are automatically created. You can limit which drivers are installed by using the driver compatibility list.

### Limiting Printing Bandwidth in ICA Sessions

When users access MetaFrame XP servers through slower networks or dial-up connections, data sent during printing can affect video updates and application performance. To achieve the best performance for some users, you can limit the bandwidth used by print data streams in ICA sessions.

By limiting the data transmission rate for printing, you make more bandwidth available in the ICA data stream for transmission of video, keystrokes, and mouse data. More available bandwidth can help prevent degradation of the user experience during printing.

Use the Management Console for MetaFrame XP to limit printing bandwidth in the server farm. You can set limits on individual servers and copy the bandwidth setting from one server to one or more other servers.

You can monitor the current bandwidth setting when you select the Printer Management node or the Servers node in the console tree. For more information about views for bandwidth management, see “Using the Printer Management Node” on page 295 and “Bandwidth Tab” on page 297.
MetaFrame XP Commands

This appendix describes MetaFrame XP commands. These commands must be run from the command prompt on a MetaFrame XP server. They provide additional methods for maintaining and configuring MetaFrame XP servers and server farms.

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>acrcfg</td>
<td>Configure autoreconnect settings</td>
</tr>
<tr>
<td>altaddr</td>
<td>Specify server alternate IP address</td>
</tr>
<tr>
<td>app</td>
<td>Run application execution shell</td>
</tr>
<tr>
<td>apputil</td>
<td>Add servers to Configured Servers list for published applications</td>
</tr>
<tr>
<td>auditlog</td>
<td>Generate server logon/logoff reports</td>
</tr>
<tr>
<td>change client</td>
<td>Change ICA Client device mapping</td>
</tr>
<tr>
<td>chfarm</td>
<td>Change the server farm membership of the server</td>
</tr>
<tr>
<td>clicense</td>
<td>Maintain MetaFrame XP licenses</td>
</tr>
<tr>
<td>cltprint</td>
<td>Set the number of ICA Client printer pipes</td>
</tr>
<tr>
<td>ctxxmlss</td>
<td>Change the XML Service port number</td>
</tr>
<tr>
<td>driveremap</td>
<td>Remap the server’s drive letters</td>
</tr>
<tr>
<td>dscheck</td>
<td>Validate the server farm’s data store’s integrity</td>
</tr>
<tr>
<td>dsmaint</td>
<td>Configure the server farm’s data store</td>
</tr>
<tr>
<td>icaport</td>
<td>Configure TCP/IP port number</td>
</tr>
<tr>
<td>imaport</td>
<td>Change IMA ports</td>
</tr>
<tr>
<td>migratetomsde</td>
<td>Migrate the server farm’s data store from a Microsoft Access database to an MSDE database</td>
</tr>
</tbody>
</table>
### Command Description

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>mlicense</td>
<td>Add multiple MetaFrame licenses to the server farm’s data store</td>
</tr>
<tr>
<td>query</td>
<td>View information about server farms, processes, servers, ICA sessions, and users</td>
</tr>
<tr>
<td>twconfig</td>
<td>Configure ICA display settings</td>
</tr>
</tbody>
</table>
ACRCFG

Use `acrcfg` to configure automatic client reconnection settings on a MetaFrame XP server or server farm.

**Syntax**

```
acrcfg [ /server:servername | /farm ] [ /query | /q ]
acrcfg [ /server:servername | /farm ] [ /require:on | off ] [ /logging:on | off ]
acrcfg [ /server:servername ] [ /inherit:on | off ] [ /require:on | off ]
   [ /logging:on | off ]
acrcfg [/?]
```

**Parameters**

*servername*

The name of a MetaFrame XP server.

**Options**

* /query, /q
  
  Query current settings.

* /server
  
  The server to be viewed or modified by the other command line options. The server specified by `servername` must be in the same server farm as the server on which the command is run. This option and the `/farm` option are mutually exclusive. The local server is the default if neither `/server` nor `/farm` is indicated.

* /farm
  
  The options on the command line after `/farm` are applied to the entire server farm.

* /inherit:on | off
  
  To use the auto client reconnect settings from the server farm set `/inherit` to `on` for a server. To disregard the server farm auto client reconnect settings, set `/inherit` to `off`. By default, `/inherit` is set to `on` for a server.

* /require:on | off
  
  If you want users to be prompted for credentials during automatic reconnection, set `/require` to `on`. Servers inherit the server farm setting unless `/inherit` is `off`. To allow users to automatically reconnect to disconnected sessions without providing credentials, set `/require` to `off`. By default, `/require` is set to `off` for both a server and a server farm.
/logging: on | off
You can enable logging of client reconnections in the Application Event Log on a server. Logging can be set only when /required is set to off. Logging is set to off for both servers and server farms by default.

/?
Displays the syntax for the utility and information about the utility’s options.

Remarks
Enabling automatic client reconnection allows users to resume working where they were interrupted when an ICA connection is broken. Automatic reconnection detects broken connections, disconnects the ICA sessions involved, and then reconnects the users to their sessions.

However, automatic reconnection can result in a new ICA session being launched (instead of reconnecting to an existing session) if a client’s cookie, containing the key to the session ID and credentials, is not used. The cookie is not used if it has expired, for example, because of a delay in reconnection, or if credentials must be re-entered because /require is set to on. Auto client reconnection is not triggered if users intentionally disconnect.

The auto client reconnect feature is enabled by default and can be disabled using Appsrv.ini or an ICA file only on the ICA Win32 Client or with the Web Interface for MetaFrame XP.

The /require and /logging options are valid with either /server or /farm, but /inherit is not used with /farm. If neither /server nor /farm is selected and the /inherit, /require, or /logging options are used, they are applied to the local server. You can set /require only when /inherit is set to off. You can set logging only when /require and /inherit are set to off. When logging is not valid it disappears from later queries. A query shows the require setting whether or not it is on.

Settings and values are not case sensitive.

Examples
The following four commands result in the following configurations:
• Require users to enter credentials when they automatically reconnect to servers configured to inherit farm-wide settings
• Show the results
• Allow users to be re-authenticated automatically to the local server and set the server to log client reconnections
• Show the results

C:\>acrcfg /farm /require:on
Update successful
C:\>acrcfg /farm /q
Auto Client Reconnect Info for: Farm-wide Settings
REQUIRE: on
C:\>acrcfg /inherit:off /require:off /logging:on
Update successful
C:\>acrcfg /q
Auto Client Reconnect Info for: Local Server
INHERIT: off
REQUIRE: off
LOGGING: on

Security Restrictions

You must be a MetaFrame XP administrator to make changes.
ALTADDR

Use **altaddr** to query and set the alternate (external) IP address for a MetaFrame XP server. The alternate address is returned to ICA Clients that request it and is used to access a MetaFrame XP server that is behind a firewall.

**Syntax**

```
altaddr [/server:servername] [/set alternateaddress ] [/v]
altaddr [/server:servername] [/set adapteraddress alternateaddress] [/v]
altaddr [/server:servername] [/delete] [/v]
altaddr [/server:servername] [/delete adapteraddress] [/v]
altaddr [/?]
```

**Parameters**

- **servername**
  - The name of a MetaFrame XP server.

- **alternateaddress**
  - The alternate IP address for a MetaFrame XP server.

- **adapteraddress**
  - The local IP address to which an alternate address is assigned.

**Options**

- **/server:servername**
  - Specifies the MetaFrame XP server on which to set an alternate address. Defaults to the current MetaFrame XP server.

- **/set**
  - Sets alternate TCP/IP addresses. If an **adapteraddress** is specified, **alternateaddress** is assigned only to the network adapter with that IP address.

- **/delete**
  - Deletes the default alternate address on the specified server. If an adapter address is specified, the alternate address for that adapter is deleted.

- **/v (verbose)**
  - Displays information about the actions being performed.

- **/?**
  - Displays the syntax for the utility and information about the utility’s options.
Remarks
The MetaFrame server subsystem reads the altaddr settings for server external IP addresses at startup only. If you use altaddr to change the IP address setting, you must restart the IMA service for the new setting to take effect. However, if you restart the IMA service when the MetaFrame server has active ICA sessions, you will disconnect the ICA sessions.

If altaddr is run without any parameters, it displays the information for alternate addresses configured on the current server.

Examples
Set the server’s alternate address to 1.1.1.1:
altaddr /set 1.1.1.1

Set the server’s alternate address to 2.2.2.2 on the network interface card whose adapter address is 1.1.1.1:
altaddr /set 2.2.2.2 1.1.1.1

Security Restrictions
None.
**APP**

*App* is a script interpreter for secure application execution. Use *App* to read execution scripts that copy standardized “.ini” type files to user directories before starting an application, or to perform application-related cleanup after an application terminates. The script commands are described below.

**Syntax**

```
app scriptfilename
```

**Parameter**

*scriptfilename*

The name of a script file containing app commands (see script commands below).

**Remarks**

If no *scriptfilename* is specified, *app* displays an error message.

The Application Execution Shell reads commands from the script file and processes them in sequential order. The script file must reside in the %SystemRoot%\Scripts directory.

**Script Commands**

The script commands are:

- **copy** sourcedirectory\filespec targetdirectory
  - Copies files from *sourcedirectory* to *targetdirectory*. *Filespec* specifies the files to copy and can include wild cards (*,?).

- **delete** directory\filespec
  - Deletes files owned by a user in the *directory* specified. *Filespec* specifies the files to delete and can include wild cards (*,?). See the Examples section for more information.

- **deleteall** directory\filespec
  - Deletes all files in the *directory* specified.

- **execute**
  -Executes the program specified by the path command using the working directory specified by the *workdir* command.

- **path** executablepath
  - *Executablepath* is the fully qualified name of the executable to be run.
workdir directory
Sets the default working directory to the path specified by directory.

Script Parameters

directory
A directory or directory path.

executablepath
The fully qualified name of the executable to be run.

filespec
Specifies the files to copy and can include wildcards (*,?).

sourcedirectory
The directory and path from which files are to be copied.

targetdirectory
The directory and path to which files are to be copied.

Examples

The following script file runs the program Sol.exe:

```
PATH C:\Wtsrv\System32\Sol.exe
WORKDIR C:\Temp
EXECUTE
```

The following script file runs the program Notepad.exe. When the program terminates, the script deletes files in the Myapps\Data directory created for the user who launched the application:

```
PATH C:\Myapps\notepad.exe
WORKDIR C:\Myapps\Data
EXECUTE
DELETE C:\Myapps\Data\*.*
```

The following script file copies all the Wri files from the directory C:\Write\Files, executes Write.exe in directory C:\Temp.wri, and then removes all files from that directory when the program terminates:

```
PATH C:\Wtsrv\System32\Write.exe
WORKDIR C:\Temp.wri
COPY C:\Write\Files\*.wri C:\Temp.wri
EXECUTE
DELETEALL C:\Temp.wri\*.*
```
The following example demonstrates using the script file to implement a front-end registration utility before executing the application Coolapp.exe. You can use this method to run several applications in succession:

```
PATH C:\Regutil\Reg.exe
WORKDIR C:\Regutil
EXECUTE
PATH C:\Coolstuff\Coolapp.exe
WORKDIR C:\Temp
EXECUTE
DELETEALL C:\Temp
```

**Security Restrictions**

None.
APPUTIL

Use `apputil` to add servers to the Configured Servers list for a published application.

Syntax

```
apputil [/? ]
apputil [/q ]
apputil [/i applicationID servername ]
apputil [/u applicationID servername ]
```

Parameters

`applicationID`

The ID of a published application, as displayed by the `/q` option.

`servername`

The name of the server to add to the Configured Servers list for the published application.

Options

`/?`

Display the syntax for the utility and information about the utility’s options.

`/q`

Query a list of all available published applications, published desktops, and published applications bundles into Installation Manager packages.

`/i`

Add a server to the Configured Servers list for a specified published application.

You can use the `/i` option with the following types of published resources:

- **Standard published applications.** Note that any server-specific overrides you configured when you published the application (such as overrides to the command line and working directory entries) are not applied to the specified server when it is added to the Configured Servers list. To use the `/i` option with the published application, be sure that the target application is located in the default location you specified when you published the application.

- **Published server desktops.**

- **Installation Manager packages.** When you run `apputil` for published applications associated with Installation Manager packages, the packaged
application is scheduled for immediate installation on the target host, and the server is added to the Configured Servers list for the published application.

\texttt{/u}

Remove a server from the Configured Servers list for a specified Published Application. Note that if the application published an Installation Manager package, then that package is not uninstalled from the target host.

**Remarks**

When using the \texttt{/i} option with an Installation Manager package, an unnamed Installation Manager job is created. When the job is successfully completed, connections to the published application are enabled on the server.

When you manually add servers to the Configured Servers list for Installation Manager packages in the Management Console, you are presented with a dialog box allowing you to schedule the installation time for the package. However, when you run the \texttt{apputil} utility, installation is scheduled immediately.

If an error occurs during execution of the utility, the process exit code “1.0” is returned on success.

You must run this utility from a Metaframe XPe server running MetaFrame XP with Feature Release 3 or later and Installation Manager.

**Examples**

The following example displays the correct syntax and usage for the \texttt{apputil} utility.

C:\>apputil /q
Available published applications: 3.
Application ID Type Description
2e0e-0009-000010a9 Application Word
2e0e-0009-000010ac Desktop Desktop
2e0e-0009-000010af Package Acrobat Reader

C:\>apputil /i 2e0e-0009-000010a9 PLEIONE
Success. The published application is now configured for the specified server.

C:\>apputil /i 2e0e-0009-000010ac PLEIONE
Success. The published desktop is now configured for the specified server.

C:\>apputil /i 2e0e-0009-000010af PLEIONE
Success. The packaged application has been scheduled for immediate installation.
Running the following script adds a server (specified as a command line parameter), to the Configured Servers list for a published application.

Script name: Rollout.cmd

```
AppUtil.exe /i 397e-0009-00000430 %1
@IF ERRORLEVEL 1 goto Error
AppUtil.exe /i 397e-0009-00000491 %1
@IF ERRORLEVEL 1 goto Error
AppUtil.exe /i 397e-0009-00000494 %1
@IF ERRORLEVEL 1 goto Error
AppUtil.exe /i 397e-0009-0000049a %1
@IF ERRORLEVEL 1 goto Error
@ECHO Success!
@GOTO End
:Error
@ECHO Failure!
:End
Usage: Rollout.cmd <server>
```

**Security Restrictions**

To run this utility, you must be a MetaFrame XP administrator with the right to carry out the following tasks:

- To use the /q option, you must at least have the right to view published applications and content.
- To use the /i or /u options for published applications and published desktops, you must have the right to view published applications, to publish applications, and to edit a published application’s properties.
- To use the /i option for Installation Manager packaged applications, you must have the right to edit Installation Manager, in addition to the rights described above.
AUDITLOG

Auditlog generates reports of logon/logoff activity for a MetaFrame server based on the Windows NT Server security event log. To use auditlog, you must first enable logon/logoff accounting. You can direct the auditlog output to a file.

Syntax

auditlog [username | session] [eventlog:filename] [before:mm/dd/yy]
   [after:mm/dd/yy] [write:filename] [detail | time] [all]

Parameters

filename
The name of the eventlog output file.

session
Specifies the session ID for which to produce a logon/logoff report. Use this parameter to examine the logon/logoff record for a particular session.

mm/dd/yy
The month, day, and year (in two-digit format) to limit logging.

username
Specifies a username for which to produce a logon/logoff report. Use this parameter to examine the logon/logoff record for a particular user.

Options

/eventlog:filename
Specifies the name of a backup event log to use as input to auditlog. You can back up the current log from the Event Log Viewer by using auditlog /clear:filename.

:before:mm/dd/yy
Reports on logon/logoff activity only before mm/dd/yy.

/after:mm/dd/yy
Reports on logon/logoff activity only after mm/dd/yy.
**/write:** *filename*

Specifies the name of an output file. Creates a comma-delimited file that can be imported into an application, such as a spreadsheet, to produce custom reports or statistics. It generates a report of logon/logoff activity for each user, displaying logon/logoff times and total time logged on.

If *filename* exists, the data is appended to the file.

**/time**

Generates a report of logon/logoff activity for each user, displaying logon/logoff times and total time logged on. Useful for gathering usage statistics by user.

**/fail**

Generates a report of all failed logon attempts.

**/all**

Generates a report of all logon/logoff activity.

**/detail**

Generates a detailed report of logon/logoff activity.

**/clear:** *filename*

Saves the current event log in *filename* and clears the event log. This command does not work if *filename* already exists.

**/?**

Displays the syntax for the utility and information about the utility’s options.

**Remarks**

*Auditlog* provides logs you can use to verify system security and correct usage. The information can be extracted as reports or as comma-delimited files that can be used as input to other programs.

You must enable logon/logoff accounting on the local server to collect the information used by *auditlog*. To enable logon/logoff accounting, log on as a local administrator and enable logon/logoff accounting with User Manager for Domains (Windows NT) or with Audit Policy in Microsoft Management Console (Windows 2000).

**Security Restrictions**

None.
CHANGE CLIENT

Change client changes the current disk drive, COM port and LPT port mapping settings for an ICA Client device.

Syntax

change client [/view | /flush | /current]
change client [{/[default | /[default_drives] | /[default_printers]]} /[ascending]]
change client [/default | [/default_drives] | [/default_printers]} [/ascending]
change client [/noremap] [/persistent] [/force_prt_todef]
change client [/delete host_device] [host_device client_device] [/?]

Parameters

host_device
The name of a device on the host server to be mapped to a client device.

client_device
The name of a device on the client to be mapped to host_device.

Options

/view
Displays a list of all available client devices.

/flush
Flushes the client drive mapping cache. This action forces the server and the client to resynchronize all disk data. See Remarks for more information.

/current
Displays the current ICA Client device mappings.

/default
Resets host drive and printer mappings to defaults.

/default_drives
Resets host drive mappings to defaults.

/default_printers
Resets host printer mappings to defaults.

/ascending
Uses ascending, instead of descending, search order for available drives and printers to map. This option can be used only with /default, /default_drives, or /default_printer.
/noremap
   If /noremap is specified, client drives that conflict with MetaFrame drives are
   not mapped.

/persistent
   Saves the current client drive mappings in the client device user’s profile.

/force_prt_todef
   Sets the default printer for the client session to the default printer on the
   client’s Windows desktop.

/delete host_device
   Deletes the client device mapping to host_device.

/? (help)
   Displays the syntax for the utility and information about the utility’s options.

Remarks
Typing change client with no parameters displays the current ICA Client device
mappings; it is equivalent to typing change client /current.

Use change client host_device client_device to create a client drive mapping. This
maps the client_device drive letter to the letter specified by host_device; for
example, change client v: c: maps client drive C to drive V on the MetaFrame
server.

The /view option displays the share name, the share type, and a comment describing
the mapped device. Sample output for change client /view follows:

C:>change client /view
Available Shares on client connection ICA-tcp#7

<table>
<thead>
<tr>
<th>Sharename</th>
<th>Type</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>\Client\A:</td>
<td>Disk</td>
<td>Floppy</td>
</tr>
<tr>
<td>\Client\C:</td>
<td>Disk</td>
<td>FixedDrive</td>
</tr>
<tr>
<td>\Client\D:</td>
<td>Disk</td>
<td>CdRom</td>
</tr>
<tr>
<td>\Client\LPT1:</td>
<td>Printer</td>
<td>Parallel Printer</td>
</tr>
<tr>
<td>\Client\COM1:</td>
<td>Printer</td>
<td>Serial Printer</td>
</tr>
</tbody>
</table>
The /flush option flushes the client drive cache. This cache is used to speed up access to client disk drives by retaining a local copy of the data on the MetaFrame server. The time-out for hard drive cache entries is ten minutes and the time-out for diskette data is five seconds. If the client device is using a multitasking operating system and files are created or modified, the MetaFrame server does not know about the changes.

Flushing the cache forces the data on the MetaFrame server to be synchronized with the client data. The cache time-out for diskettes is set to five seconds because diskette data is usually more volatile; that is, the diskette can be removed and another diskette inserted.

The /default option maps the drives and printers on the client device to mapped drives and printers on the MetaFrame server. A and B Drives are always mapped to drives A and B on the MetaFrame server. Hard drives are mapped to their corresponding drive letters if those drive letters are available on the MetaFrame server. If the corresponding drive letter is in use on the MetaFrame server, the default action is to map the drive to the highest unused drive letter. For example, if both machines have drives C and D, the client drives C and D are mapped to V and U respectively. These default mappings can be modified by the /ascending and /noremap options.

The /default_printers option resets printer mappings to defaults. /default_printers attempts a one-to-one mapping of all client printers; for example, the client’s LPT1 and LPT2 ports are mapped to the server’s LPT1 and LPT2 ports. If the /ascending option is specified, the mapping is done in ascending order.

The /default_drives option resets host drive mappings to defaults. /default_drives attempts a one-to-one mapping of all client drives; for example, client drives A and B are mapped to server drives A and B. Hard drives are mapped to their corresponding drive letters if those drive letters are available on the MetaFrame server. If the corresponding drive letter is in use on the MetaFrame server, the default action is to map the drive to the highest unused drive letter. For example, if both machines have drives C and D, the client drives C and D are mapped to V and U respectively. If the /ascending option is specified, the mapping is done in ascending order.

The /ascending option causes the mapping to occur in ascending drive letter order. For example, if the first two available drive letters on the MetaFrame server are I and J, drives C and D in the preceding example are mapped to I and J respectively.

The /noremap option causes the mapping to skip drive letters occupied on the MetaFrame server. For example, if the MetaFrame server has a C drive but no D drive, the client’s C drive is mapped to D on the server, but the client’s D drive is not mapped.

The /persistent option causes the current device mappings to be saved in the user’s profile. Drive conflicts can occur if the /persistent option is in use, and the user
logs on from a client device that has a different disk drive configuration, or logs on to a MetaFrame server that has a different disk drive configuration.

The /force_prt_todef option sets the default printer for the ICA session to the default printer on the client’s Windows desktop.

**Security Restrictions**

None.
CHFARM

Change farm is used to change the farm membership of a MetaFrame XP server.

Syntax

chfarm

Remarks

You can use chfarm when you want to move a MetaFrame XP server from its current server farm. You can move the server to an existing IMA-based server farm or create a new server farm at the same time that you move the server. Citrix recommends that you back up your data store before running chfarm.

Important If the server you want to move provides information for a Resource Manager summary database, update the summary database before using chfarm. If you do not update the summary database, you will lose approximately 24 hours worth of summary data stored on the server. To update the summary database, click the Resource Manager node in the Management Console for MetaFrame XP, select the Summary Database tab, and click Update Now.

The chfarm utility is installed in %ProgramFiles%\citrix\system32\citrix\IMA. To run this utility, choose Run from the Start menu. Enter chfarm.

Warning Be sure that the Management Console is closed before you run the chfarm command. Running chfarm while the console is open can result in loss of data and functionality.

Chfarm stops the IMA service on the server. The data store configuration part of the MetaFrame XP Setup wizard appears. On the first page, you can select to join an existing server farm or create a new server farm.

The wizard continues and you specify an existing data store (to join an existing server farm) or set up a new data store (if you create a new server farm). While running chfarm, you are prompted for the user name and password of the user you want to designate as the initial MetaFrame XP administrator for the farm. For information about data store setup and server farm configuration, see “Configuring the Data Store” on page 116.

If chfarm reports any error, continuing the process can corrupt the data store. If you cancel out of the data store configuration part of the MetaFrame XP Setup wizard, the server you are switching rejoins the original farm.
After the farm membership is changed or a new farm is created, reboot the MetaFrame XP server.

Do not remove a server that hosts a server farm’s data store from the server farm. Doing so renders the farm unstable.

**Important Notes for Using MSDE for the Data Store**

This section explains how to use `chfarm` to create a new farm — which uses Microsoft SQL Server 2000 Database Engine (MSDE) for the server farm’s data store — when changing a MetaFrame XP server’s farm membership.

If you want to use MSDE to host a new server farm’s data store, a named instance of MSDE must be installed on the server on which you run `chfarm`. The default named instance that `chfarm` uses is CITRIX_METAFRAME.

Running `chfarm` does not automatically install MSDE; you must install it separately. For information about installing MSDE on the MetaFrame XP server, see “Microsoft SQL Server 2000 Desktop Engine (MSDE)” on page 56.

**Chfarm Options When Using MSDE**

Use these options when running `chfarm` to create a new farm with MSDE as the data store:

- `/instancename:<name>`
  The name of the MSDE instance to which to migrate. The default value is CITRIX_METAFRAME.

- `/database:<name>`
  The name of the MSDE database to which to migrate. The default value is MF20.

**Note** You cannot migrate a database to the same named instance of MSDE that is already in use. If you are already using MSDE and you want to migrate to a new farm using MSDE, you must either migrate to another database (Access or a third party database) and then back to MSDE, or install another named instance of MSDE and then launch `chfarm` with the `/instancename` option.

- **To move a server to a new server farm using MSDE as the data store**
  1. Create a named instance of MSDE by installing MSDE on the first server in the new farm.
  2. Run `chfarm` on the server that you want to use to create the new farm using the `/instancename:<name>` option, where `<name>` is the name of the instance of MSDE you created in Step 1.
Note If you named an instance of MSDE “CITRIX_METAFRAME,” you do not need to use the /instancename option.
CLICENSE

You can use `clicense` to add, remove, query, and maintain license information for MetaFrame XP servers within a server farm. For more information about MetaFrame XP licensing, see “Licensing MetaFrame XP” on page 137.

Syntax

```plaintext
clicense [add serial_number]
clicense [remove license_string]
clicense [force_remove license_string]
clicense [activate license_string activation_code]
clicense [assign license_set_id server_name number_to_assign]
clicense [strings]
clicense [products]
clicense [connections]
clicense [servers_using license_set_id]
clicense [in_use_by server_name]
clicense [in_set license_set_id]
clicense [sets_in license_string]
clicense [assigned_to server_name]
clicense [servers_assigned license_set_id]
clicense [available_for_assignment license_set_id]
clicense [read_db [file_name]]
clicense [refresh]
clicense [help option]
```

Parameters

- `activation_code`
  The license activation code. This is obtained from the Citrix Product Activation System (http://www.citrix.com/activate).

- `file_name`
  The name of the licensing database file.

- `option`
  The name of a `clicense` option.
license_string
The license number. A license number consists of seven groups of five characters each: xxxxx-xxxxx-xxxxx-xxxxx-xxxxx-xxxxx-xxxxx. Each license number has an associated serial number which consists of five groups of five characters each: xxxxx-xxxxx-xxxxx-xxxxx-xxxxx.

license_set_id
The license set ID number.

number_to_assign
The number of license counts to assign to a specified server.

serial_number
The license serial number. This number is located on the software packaging. See license_string.

server_name
The name or IP address of a MetaFrame XP server. Use a period (.) to specify the local server.

Options

add serial_number
Use to add serial numbers to the license store. This returns the added license string.

remove license_string
Use to remove a license string from the license store, provided it does not have active assignments.

force_remove license_string
Use to force the removal of a license string from the license store. Active assignments are dropped.

activate license_string activation_code
Activates a license string in the license store.

assign license_set_id server_name number_to_assign
Assigns licenses from the specified license set to the specified MetaFrame XP server. To specify the local server, enter a period (.).

strings
Retrieves a list of all installed license strings.

products
Retrieves a list of all the installed product licenses.

connections
Retrieves a list of all installed connection licenses.
servers_using license_set_id
    Retrieves a list of all servers that are using a license from the specified license set.

in_use_by server_name
    Queries and returns the license sets currently in use by the specified server.

in_set license_set_id
    Returns a list of all strings that contribute licenses to a set.

sets_in license_string
    Returns a list of all license sets to which a string contributes.

assigned_to server_name
    Returns the license sets that are assigned to the specified server.

servers_assigned license_set_id
    Returns the servers to which the specified license set is assigned.

available_for_assignment license_set_id
    Returns the number of activated licenses in a license set that can be assigned.

read_db [file_name]
    Reads license database configuration files into the license store. If a file name is specified, only files whose names begin with the specified file name are read into the license store.

refresh
    Refreshes all licensing data.

clickense option
    Provides additional information about the specified option.

Remarks
Citrix Management Console provides a graphical user interface with the same functionality as the clicense command for managing MetaFrame XP licenses.

Security Restrictions
The clicense commands can be executed only by a member of the MetaFrame XP administrators group.
CLTPRINT

Use cltprint to set the number of printer pipes for the client print spooler.

Syntax
cltprint [/q] [/pipes:nn] [/?]

Options
/q
Displays the current number of printer pipes.

/pipes:nn
Sets the specified number of printer pipes. This number represented by nn must be from 10 to 63.

/?
Displays the syntax for the utility and information about the utility’s options.

Remarks
Printer pipes are used to send data from applications to client print spoolers. The number of pipes specifies the number of print jobs that can be sent to the spooler simultaneously.

The default number of printer pipes is ten.

The Spooler service must be stopped and restarted after changing the number of pipes. Print jobs already spooled continue printing.

Print jobs sent to the spooler trigger an error message while the service is stopped. Make sure no users start printing during the time the Spooler service is stopped.

Security Restrictions
None.
CTXMLSS

Use **ctxxmlss** to change the Citrix XML Service port number.

**Syntax**

ctxxmlss [/r nnn] [/u] [/k nnn] [/?]

**Options**

/r nnn
   Changes the port number for the Citrix XML Service to nnn.

/u
   Unloads Citrix XML Service from memory.

/k nnn
   Keeps the connection alive for nnn seconds. The default is nine seconds.

/?
   Displays the syntax for the utility and information about the utility’s options.

**Remarks**

For more information, see “Configuring the Citrix XML Service Port” on page 125.

**Security Restrictions**

None.
DRIVEREMAP

Use the **driveremap** utility to change the MetaFrame XP server’s drive letters. MetaFrame XP Setup installs the **driveremap** utility in C:\Program Files\Citrix\System32.

---

**Note** In previous releases of MetaFrame, the utility to change the server’s drive letters was named drvremap.exe.

---

**Important** If you are installing MetaFrame XP on a server that is not running a previous version of MetaFrame, run the **driveremap** utility before you install MetaFrame XP. Citrix recommends that you do not change server drive letters after you install MetaFrame XP and any applications you want to publish for users to access.

---

**Syntax**

```
driveremap /?
driveremap /drive:M
driveremap /u
driveremap /noreboot
driveremap /IME
```

**Options**

The following parameters can be used with driveremap at a command line.

```
/?
```

Displays the syntax for the utility and information about the utility’s options.

```
/drive:M
```

Specifies the drive letter to use for the first remapped drive.

```
/u
```

Permits unattended or silent installation where no dialog boxes are displayed and no user input is required. You must use this option in conjunction with the /drive: option.

```
/noreboot
```

Surpresses the **Restart Computer** message and does not restart the system. Citrix strongly recommends that you restart the system after running this utility.
/ime[filename]

Changes the drive letter specified in
Software\Microsoft\Windows\CurrentVersion\Ime\Japan\IMEJP\Dictionaries
for all of the loaded hives under HKEY_USERS.

Remarks

The **driveremap** utility has a user interface that allows you to select the drive letters
you want to map. The user interface is available from the MetaFrame XP CD’s
Autorun screen and when you run Driveremap.exe with no command line
parameters.

Examples

The following command remaps the server’s drive letters. The first available drive
is changed to M. The command uses the **noreboot** option, which suppresses the
appearance of any dialog boxes.

**driveremap /u /drive:M /noreboot**

The following command changes the server’s drive letters back to the drive letters
that start at C and then prompts you to restart the server.

**driveremap /u /drive:M /drive:C**

Known Issues

The following items are known issues you may encounter when running the **driveremap** utility.

- When running **driveremap** with no parameters, the drive letter choices in the
drop-down list may be greyed out. This can occur if the server has non-
contiguous drive letters, for example, C, D, X. The mapped drive letters are
spread over the interval [a..z] and no reasonable interval shifting can be
performed. Network drives are also taken into account.

  To work around this issue, change the drive letters to C, D, and E and then run
  the **driveremap** utility.

- At the command prompt, if you remap to a letter that is in use, nothing happens
and you are returned to the prompt. Locate the server’s drive letters in Windows
Explorer to verify that the drive letters are changed.

- MetaFrame XP server drive remapping is not supported on Windows 2000
Dynamic Disks.

- Installation of the Web Interface for MetaFrame XP on a MetaFrame XP server
may fail if you are upgrading a server with remapped drives. See article
CTX240747 in the online Citrix Knowledge Base at
http://www.citrix.com/support for more information.
If you upgrade from MetaFrame 1.8 to MetaFrame XP on a server with changed server drive letters, the ICA Win32 Pass-Through Client is not updated. To avoid this issue, be sure the server is operating in install mode before running Setup.

Security Restrictions

Only MetaFrame XP administrators can execute this command.
DSCHECK

Use dscheck to validate the consistency of the database used to host the MetaFrame server farm’s data store. You can then repair any inconsistencies found.

Syntax

dscheck [/clean] [/?] 

Options

/clean
Attempts to fix any consistency error that is found.

/?
Displays the syntax for the utility and information about the utility’s options.

Remarks

Dscheck performs a variety of tests to validate the integrity of a MetaFrame XP farm’s data store. When run without parameters, only these tests are run. Run dscheck on a server in the farm that has a direct connection to the data store.

When you run dscheck with the /clean option, the utility runs tests and removes inconsistent data (typically servers and applications) from the data store. Because removing this data can affect the farm’s operation, be sure to back up the data store before using the /clean option. You can restore the data you backed up. Contact Citrix Technical Support for further assistance.

When you run the utility with the /clean option, you may need to run the dsmaint command with the recreatelhc parameter on each server in the farm to update the local host caches. Running this command sets the PSRequired registry value to 1 in HKLM\SOFTWARE\Citrix\IMA\Runtime.

Dscheck reports the results of the tests in several ways. First, dscheck sends any errors found as well as a summary to the event log and to the command window. You can also write the output produced by dscheck to a file.

Second, several performance monitor values are updated under the Citrix MetaFrame XP performance object. These values include a count of server errors, a count of application errors, a count of group errors, and an overall flag indicating that errors were detected. The performance monitor values can be used with Resource Manager to detect when problems are present.

Third, dscheck returns an error code of 0 for a successful scan (no errors were found) and an error code of 1 if any problems are encountered.
Dscheck looks primarily at three data store objects: servers, applications, and groups. For each of these object types, dscheck performs a series of tests on each object instance.

For example, for each MetaFrame server object in the data store, dscheck verifies that there is a corresponding common server object and then further verifies that both objects have matching host IDs and host names.

**Examples**

To run consistency checks only:

```
dscheck
```

To check consistency and fix errors:

```
dscheck /clean
```

**Security Restrictions**

To run this utility, you must have direct access to the data store.
DSMAINT

Use **dsmaint** to configure the IMA data store for a MetaFrame XP server farm.

When using this command, user names and passwords may be case-sensitive, depending on the database product you are using and the operating system it runs on.

**Syntax**

```
 dsmaint config [user:username] [pwd:password] [dsn:filename]
 dsmaint backup destination_path
 dsmaint failover direct_server
 dsmaint compactdb [ds] [lhc]
 dsmaint migrate [{srcdsn:dsn1 /srcuser:user1 /srcpwd:pwd1}] [{dstdsn:dsn2 /dstuser:user2 /dstdpwd:pwd2}]
 dsmaint publishsqlds /user:username /pwd:password
 dsmaint recover
 dsmaint recreatelhc
 dsmaint [/?]
```

**Parameters**

`destination_path`
- Path to the backup data store.

`dsn1`
- The name of the source data store.

`dsn2`
- The name of the destination data store

`filename`
- The name of the data store.

`direct_server`
- The name of the new direct server for IMA data store operations.

`password`
- The password to connect to the data store.

`pwd1`
- The source data store password.
pwd2
The destination data store password.

user1
The source data store user logon.

user2
The destination data store user logon.

username
The name of the user to use when connecting to the data store.

Options

cfg
Changes configuration parameters used by IMA to connect to the data store.

/config
Changes configuration parameters used by IMA to connect to the data store.

/usr:username
The username to connect to a data store.

/pwd:password
The password to connect to a data store.

/dsn:filename
The filename of an IMA data store.

backup
Creates a backup copy of the Access database that is the farm’s data store. Run this command on the server that hosts the data store. Requires a path or share point to which the database file will be copied. The backup command cannot be used to create backups for Oracle or SQL data stores.

failover
Switches the server to use a new direct server for IMA data store operations.

compactdb
Compacts the Access database file.

/ds
Compacts the Access database file. If the IMA service is running, this can be executed from the direct server or an indirect server. If the IMA service is not running, this can be executed only on the direct server.

/lhc
Compacts the local host cache.

migrate
Migrate data from one data store to another. Use this command to move a data store to another server, rename a data store in the event of a server name change, or migrate the data store to an Oracle or SQL Server database.
/srcdsn:dsn1  
The name of the data store from which to migrate data.

/srcuser:user1  
The user name to use to connect to the data store from which the data is migrating.

/srcpwd:pwd1  
The password to use to connect to the data store from which the data is migrating.

/dstdsn:dsn2  
The name of the data store to which to migrate the data.

/dstuser:user2  
The user name that allows you to connect to the data store to which you are migrating the source data store.

/dstpwd:pwd2  
The password that allows you to connect to the data store to which you are migrating the source data store.

publishsqlds  
Publishes a MetaFrame data store to allow replication.

recover  
Restores an Access data store to its last known good state. This must be executed on the direct server while the IMA service is not running.

recreatelhc  
Recreates the local host cache database.

/?  
Displays the syntax for the utility and information about the utility’s options.

Remarks

compactdb  
During database compaction, the database is temporarily unavailable for both reading and writing. The compaction time can vary from a few seconds to a few minutes, depending on the size of the database and the usage.

config  
For Access databases, this command resets the password used to protect the database, setting the matched security context to allow IMA access to this database.

You must stop the IMA service before using config with the /pwd option.
**Warning** You must specify a /dsn for **dsmaint config** or you will change the security context for access to the SQL or Oracle database.

**migrate**
Databases can be migrated from Access to SQL or Oracle and between SQL and Oracle.

**Important** By default, the Access database does not have a user name or password. When migrating a database from Access, leave the /srcuser: and /srcpwd: parameters blank.

The connection to a local Access database is based on the host server’s name. If the name of the server changes, use **migrate** to change the name of the database.

**publishsqls**
Execute **publishsqls** only from the server that created the farm. The publication will be named **MFXPDS**.

**Security Restrictions**
The **dsmaint config** and **dsmaint migrate** commands can be executed only by a user with the correct username and password for the database.
ICAPORT

Use `icaport` to query or change the TCP/IP port number used by the ICA protocol on the MetaFrame XP server.

Syntax

```
icaport [/query | /port:nnn | /reset] [/?]
```

Options

```
/query
  Queries the current setting.

/port:nnn
  Changes the TCP/IP port number to nnn.

/reset
  Resets the TCP/IP port number to 1494, which is the default.

/?
  Displays the syntax for the utility and information about the utility’s options.
```

Remarks

The default port number is 1494. The port number must be in the range of 0–65535 and must not conflict with other well-known port numbers.

If you change the port number, restart the server for the new value to take effect. If you change the port number on the MetaFrame XP server, you must also change it on every ICA Client that will connect to that server. For instructions for changing the port number on ICA Clients, see the Citrix ICA Client Administrator’s Guide for the ICA Clients that you plan to deploy.

Examples

To set the TCP/IP port number to 5000:
```
icaport /port:5000
```

To reset the port number to 1494:
```
icaport /reset
```

Security Restrictions

Only MetaFrame XP administrators can run `icaport`.
**IMAPORT**

Use `imaport` to query or change the IMA port.

---

**Important** When you run MetaFrame XP Setup, the setup program references port 2513 for communication with the Management Console for MetaFrame XP. If you change this port number on the first server in the farm on which you install MetaFrame, you cannot join additional servers to the server farm.

---

**Syntax**

```
imaport [/query | /set {IMA:nnn | ds:nnn | cmc:nnn}* | /reset {IMA | DS | CMC | ALL}* | /?] 
```

**Options**

`/query`  
Queries the current setting.

`/set`  
Sets the designated TCP/IP port(s) to a specified port number.

- `ima:nnn`  
  Sets the IMA communication port to a specified port number.

- `cmc:nnn`  
  Sets the Management Console for MetaFrame XP connection port to a specified port number.

- `ds:nnn`  
  Sets the data store server port to a specified port number (indirect servers only).

`/reset`  
Resets the specified TCP/IP port to the default.

- `ima`  
  Resets the IMA communication port to 2512.

- `cmc`  
  Resets the Management Console for MetaFrame XP connection port to 2513.

- `ds`  
  Resets the data store server port to 2512 (indirect servers only).

- `all`  
  Resets all of the applicable ports to the defaults.
/?
Displays the syntax for the utility and information about the utility’s options.
MIGRATETOMSDE

Use `migratetomsde` to migrate a server farm’s data store from Microsoft Access to Microsoft SQL Server 2000 Database Engine (MSDE).

Migratetomsde offers fail-safe operation and automatically rolls back any changes that it makes to the system in the event of any failures.

The utility is located on the MetaFrame XP Server CD in the Support\MSDE directory.

Syntax

```
migratetomsde [/instancename:instancename | /dbname:dbname | /accessuser:user | /accesspwd:pwd | /revert | [/?]]
```

Options

`/instancename:instancename`
Specify a named instance of MSDE other than the default value of CITRIX_METAFRAME.

`/dbname:dbname`
Specify a database other than the default value of MF20.

`/accessuser:user`

`/accesspwd:pwd`
Specify the user and pwd values for your Access database, if you changed them using the Dsmaint Config utility.

`/revert`
Reverts to the Access database originally used as the server farm’s data store. Running this command restores backups that were made when the migration was initially done. Any changes made to the farm since the migration from Access to MSDE are lost.

`/?`
Displays the syntax for the utility and information about the utility’s options.
MLICENSE

Use the `mlicense` utility to add multiple licenses, activate multiple licenses, and back up licenses in a MetaFrame XP server farm.

Executing `mlicense` with no parameters displays help for the utility.

**Syntax**

- `mlicense add /I filename.txt /O filename.xml [/L number] [/Q]`
- `mlicense activate /A filename_processed.xml`
- `mlicense backup /O backupfilename.txt`
- `mlicense extract_unactivated /O filename.xml [/L <number>] [/Q]`
- `mlicense /?`

**Parameters**

- **Filename.txt**
  The name of the text file listing all of the license serial numbers to be added.

- **Filename.xml**
  The name of the output .xml file specified when using the `mlicense add` or `mlicense extract_unactivated` syntax described above. This file is uploaded to the Citrix Activation System (CAS) Multiple License Activation Web site.
  
    **Important** Avoid using Asian double-byte characters in the file name of the file to be uploaded.

- **Number**
  The maximum number of license numbers that each `filename.xml` file will contain. The maximum number that you can specify is 2000.

- **Filename_processed.xml**
  The file name of the license number and activation codes output file from the CAS Multiple License Activation Web site.

- **Backupfilename.txt**
  The file name containing a backup of the license serial numbers.

**Options**

- **add**
  Adds the license serial numbers from the `filename.txt` file to the MetaFrame farm and outputs a `filename.xml` file (or multiple files if using `/L`) to be used during the activation process. `/L` and `/Q` are optional.
Example: mlicense add /I C:\Temp\filename.txt /O C:\Temp\filename.xml
When this command is successfully completed, mlicense displays the message, “Successfully added all the serial numbers.”
You can upload the filename.xml output file(s) to the Multiple License Activation Web page on the Citrix Activation System (CAS) Web site to get an activation code.
You must be a MetaFrame XP administrator with rights to the licensing tasks to run this command.

activate
Uses the filename_processed.xml file returned from the Multiple License Activation Web page on the CAS Web site to activate the licenses in the MetaFrame farm.
Example: mlicense activate /I C:\Temp\filename_processed.xml
When this command is successfully completed, mlicense displays the message “Successfully activated all the licenses.”
You must be a MetaFrame XP administrator with rights to the licensing tasks to run this command.

backup
Saves the serial number strings from the MetaFrame farm in the backupfilename.txt file for backup and disaster recovery purposes.
Example: mlicense backup /O backupfilename.txt
You must be a MetaFrame XP administrator with at least view-only rights to the licensing tasks to run this command.

extract_unactivated
Extracts unactivated license strings from the MetaFrame XP server farm’s data store and creates filename.xml output file(s). Upload these files to the Multiple License Activation Web page on the CAS Web site to get an activation code. /L and /Q are optional.

Important Do not let MetaFrame licenses expire before activating them. The extract_unactivated command does not extract any unactivated licenses that have expired.

Example: mlicense extract_unactivated /O filename.xml
You must be a MetaFrame XP administrator with at least view-only rights to the licensing tasks to run this command.

/I
Input command used with add and activate. See the examples above for the proper syntax.
/O
Output command used with **add**, **backup**, and **extract_unactivated**. See the examples above for the proper syntax.

/L
Limits the number of license strings output to the *filename.xml* file. The maximum number of license strings that can go into any *filename.xml* output file is 2000. If the number of license strings exceeds 2000, additional XML files are created.

Use this option to change the default limit to a value less than 2000. Additional XML files are named by appending _1, _2, _3 ... to the output XML file name you specified (for example, filename_1.xml, filename_2.xml).

/L is an optional command that can be used with **add** and **extract_unactivated**.
Example: mlicense add /I filename.txt /O filename.xml /L 100
In this example, if *filename.txt* contains 250 license serial numbers, the **mlicense** tool outputs the following files:
filename_1.xml contains 100 license strings
filename_2.xml contains 100 license strings
filename_3.xml contains 50 license strings

/Q
This command allows the output file naming convention to restart. Running the command overwrites the existing files such as filename_1.xml, filename_2.xml, and filename_3.xml in the directory.

If you do not use the /Q option, the files are created using the next number available in the naming convention, such as filename_4.xml, filename_5.xml, and filename_6.xml. This command is optional and runs after /L.
Example: mlicense add /I C:\Temp\filename.txt /O C:\Temp\filename.xml /L 50 /Q
In the example above, if filename_1.xml (100 license strings), filename_2.xml (100 license strings), and filename_3.xml (50 license strings) already exist and filename.txt contains 250 license serial numbers, the **mlicense** tool outputs the following files:
filename_1.xml is overwritten and contains 50 license strings
filename_2.xml is overwritten and contains 50 license strings
filename_3.xml is overwritten and contains 50 license strings
filename_4.xml contains 50 license strings
filename_5.xml contains 50 license strings
/? Displays the syntax for the utility and information about the utility’s options.

Remarks
Mlicense does not add autoactivated licenses to the filename.xml file.
When creating the filename.txt file, be sure to use all uppercase letters.
The term “serial number” refers to license numbers before they are added to the farm. The term “license number” is synonymous with “license string” and “license key.”

Security Restrictions
The rights required to run mlicense with various options depends on the option you are running. See the definitions of the mlicense options above for detailed MetaFrame XP administrator rights requirements.

Using Mlicense to Add, Activate, and Back Up Licenses
Before you run mlicense, create a filename.txt file and save all of the license serial numbers that you want to add to the MetaFrame XP server farm. You can add descriptive text to the filename.txt file, such as section headings. The mlicense utility reads the license serial numbers in the file and then adds them to the data store.

Note Use all upper case letters when adding serial numbers to the filename.txt file.

To add, activate, and back up licenses using mlicense
1. From a command prompt, run the command parameters listed below. For example:
   C:\Documents and Settings\Administrator>mlicense add /I C:\Temp\filename.txt /O C:\Temp\filename.xml
   Avoid using Asian double-byte characters in the file name of the file to be uploaded.

   Note You can save the filename.xml file by specifying the directory path. Mlicense outputs the filename.xml file, which includes the license numbers to be used for activation.
2. Open a Web browser and navigate to the Multiple Activation page on the CAS (Citrix Activation System) Web site. Upload the filename.xml file. The Web site processes the filename.xml file and returns a filename_processed.xml file. Save the filename_processed.xml file on the server.

**Note** Detailed directions for using the CAS Web site are on the CAS Multiple License Activation Web page.

3. Run the mllicense activate command, using the filename_processed.xml file. Use the command parameters listed below; for example:

   C:\Program Files\Citrix\System32>mllicense activate /I filename_processed.xml

   The licenses are now activated in the MetaFrame farm.

4. After you activate the licenses, you can use the backup feature of mllicense to create a backup file of the licenses; for example:

   C:\Documents and Settings\Administrator>mllicense backup /O
   C:\Temp\backupfilename.txt
QUERY

Use **query** to display information about server farms, processes, servers, sessions, terminal servers, and users within the network.

Query Farm

**Syntax**

```
query farm  [server [/addr | /app | /app appname | /load]]
query farm  [/tcp ] [/ipx | /netbios ] [ /continue ]
query farm  [ /app | /app appname | /disc | /load | /process]
query farm  [/online | /online zonename]
query farm  [/offline | /offline zonename]
query farm  [/zone | /zone zonename]
query farm  [/?]
```

**Parameters**

- **appname**
  - The name of a published application.

- **server**
  - The name of a server within the farm.

- **zonename**
  - The name of a zone within the farm.

**Options**

- **farm**
  - Displays information about servers within an IMA-based server farm.

  - **server /addr**
    - Displays address data for the specified server.

  - **/app**
    - Displays application names and server load information for all servers within the farm, or for a specific server.

  - **/app appname**
    - Displays information for the specified application and server load information for all servers within the farm, or for a specific server.

  - **/continue**
Don’t pause after each page of output.

/disc
Displays disconnected session data for the farm.

/ipx
Displays IPX data for the farm.

/load
Displays server load information for all servers within the farm, or for a specific server.

/netbios
Displays NetBIOS data for the farm.

/process
Displays active processes for the farm.

/tcp
Displays TCP/IP data for the farm.

/online
Displays servers online within the farm and all zones. The data collectors are represented by the notation “D”.

/online zonename
Displays servers online within a specified zone. The data collectors are represented by the notation “D”.

/offline
Displays servers offline within the farm and all zones. The data collectors are represented by the notation “D”.

/offline zonename
Displays servers offline within a specified zone. The data collectors are represented by the notation “D”.

/zone
Displays all data collectors in all zones.

/zone zonename
Displays the data collector within a specified zone.

/?
Displays the syntax for the utility and information about the utility’s options.

Remarks

Query farm returns information for IMA-based servers within a MetaFrame XP server farm.
Security Restrictions

None.

Query Process

Syntax

query process  [ * | processid | username | sessionname | /id:nn
| programname ] [/server:servername ] [/system ]

query process  [/?]  

Parameters

*  
   Displays all visible processes.

processid  
   The three- or four-digit ID number of a process running within the farm.

programname  
   The name of a program within a farm.

servername  
   The name of a server within the farm.

sessionname  
   The name of a session, such as ica-tcp#7.

username  
   The name of a user connected to the farm.

Options

process  
   Displays information about processes running on the current server.

   process *  
      Displays all visible processes on the current server.

   process processid  
      Displays processes for the specified processid.

   process username  
      Displays processes belonging to the specified user.

   process sessionname  
      Displays processes running under the specified session name.
process /id:nn
Displays information about processes running on the current server by the specified ID number.

process programname
Displays process information associated with the specified program name.

process /server:servername
Displays information about processes running on the specified server. If no server is specified, the information returned is for the current server.

process /system
Displays information about system processes running on the current server.

/?
Displays the syntax for the utility and information about the utility’s options.

Security Restrictions
None.

Query Server

Syntax
| /addr]]
query server [/netbiosserver:x]
query server [/license | /app | /gateway | /serial | /disc | /serverfarm | /video]
query server [/continue] [/ignore] [/?]

Parameters

n
The number of times to ping a server (the default is five times), or the size of ping buffers (the default is 256 bytes).

server
The name of a server within the farm.

x
The default TCP, IPX, or NetBIOS server address.
Options

server server
  Displays transport information for the specified server.
/adrr
  Displays address information for the specified server.
/app
  Displays application names and server load for the specified server.
/continue
  Don’t pause after each page of output.
/count:n
  Number of times to ping the specified server.
/disc
  Displays disconnected session data on the current server.
/gateway
  Displays configured gateway addresses for the current server.
/ignore
  Ignore warning message about interoperability mode.
/ipx
  Displays IPX data for the current server.
/ipxserver:x
  Defines the IPX default server address.
/license
  Displays user licenses for the current server.
/load
  Displays local data on the specified server.
/netbios
  Displays NetBIOS data for the current server.
/netbiosserver:x
  Defines the NetBIOS default server address.
/ping
  Pings selected server. The default is five times.
/reset
  Resets the browser statistics on the specified server.
/serial
  Displays license serial numbers for the current server.
/serverfarm
  Displays server farm names and server load.
Appendix A  MetaFrame XP Commands

/size:n
Size of ping buffers. The default is 256 bytes.

/stats
Displays the browser statistics on the specified server.

/tcp
Displays the TCP/IP data for the current server.

/tcpserver:x
Defines the TCP/IP default server address.

/video
Displays VideoFrame data for the current server.

/?
Displays the syntax for the utility and information about the utility’s options.

Remarks

Query server displays data about the MetaFrame servers present on a network within a server farm running in interoperability mode. It shows all ICA Browser-based (servers running MetaFrame 1.8 or earlier versions) and IMA-based (servers running MetaFrame XP) servers within the farm, even if the server is not currently connected to the farm.

Security Restrictions
None.

Query Session

Syntax

query session [sessionname | username | sessionid]
query session [/?]

Parameters

servername
The name of a server within the farm.

sessionname
The name of a session, such as “ica-tcp/#7”.

sessionid
The two-digit ID number of a session.
**username**
The name of a user connected to the farm.

**Options**

**session sessionname**
Identifies the specified session.

**session username**
Identifies the session associated with the user name.

**session sessionid**
Identifies the session associated with the session ID number.

**session /server:servername**
Identifies the sessions on the specified server.

**session /mode**
Displays the current line settings.

**session /flow**
Displays the current flow control settings.

**session /connect**
Displays the current connection settings.

**session /counter**
Displays the current Terminal Services counter information.

`/?`
Displays the syntax for the utility and information about the utility’s options.

**Security Restrictions**
None.

**Query Termserver**

**Syntax**

```
query termserver [servername] [/domain:domain] [/address] [/continue]
query termserver [/?]  
```

**Parameters**

**servername**
The name of a server within the farm.

**domain**
The name of a domain to query.
Options

**termserver** *servername*
Identifies a Terminal Server.

*address*
Displays network and node addresses.

*continue*
Don’t pause after each page of output.

*domain:* *domain*
Displays information for the specified domain. Defaults to the current domain if no domain is specified.

*?*
Displays the syntax for the utility and information about the utility’s options.

Remarks

If no parameters are specified, **query termserver** lists all terminal servers within the current domain.

Security Restrictions

None.

Query User

Syntax

**query user** [ *username* | *sessionname* | *sessionid* ] [ /server:*servername* ]

**query user** [ /*?*/ ]

Parameters

*servername*
The name of a server within the farm.

*sessionname*
The name of a session, such as “ica-tcp#7”.

*sessionid*
The two-digit ID number of a session.

*username*
The name of a user connected to the farm.
Options

**user username**
Displays connection information for the specified user name.

**user sessionname**
Displays connection information for the specified session name.

**user sessionid**
Displays connection information for the specified session ID.

**user /server:servername**
Defines the server to be queried. The current server is queried by default.

/?
Displays the syntax for the utility and information about the utility’s options.

Remarks

If no parameters are specified, **query user** displays all user sessions on the current server.

Security Restrictions

None.
**TWCONFIG**

Use `twconfig` to configure ICA display settings that affect graphics performance for ICA Clients.

**Syntax**

```
twconfig [/query | /q]
twconfig [/inherit:on | off]
twconfig [discard:on | off]
twconfig [/supercache:on | off]
twconfig [/maxmem:nnn]
twconfig [/degrade:res | color]
twconfig [/notify:on | off]
twconfig [/?]
```

**Options**

/`query, /q`
Query current settings.

/`inherit:on | off`
Set to `on` to use the ICA display properties defined for the farm. Set to `off` to use the settings specified for this server. By default, this is set to `on`.

/`discard:on | off`
Discard redundant graphics operations.

/`supercache:on | off`
Use alternate bitmap caching method.

/`maxmem:nnn`
Maximum memory (in kilobytes) to use for each session’s graphics (150KB minimum, 8192KB maximum).

/`degrade:res | color`
When the `maxmem` limit is reached, degrade resolution first or degrade color depth first.

/`notify:on | off`
If `on`, users are alerted when `maxmem` limit is reached.

/`?`
Displays the syntax for the utility and information about the utility’s options.
Remarks

A MetaFrame XP server can be set to inherit its ICA display settings from the server farm ICA display settings. Use /query to display the current inherit settings. If /inherit is on, the settings displayed with /query are the server farm settings. When /inherit is off, the settings shown are for the current server only.

Twconfig can be used only to change the settings on this server, for this server. To change the settings for another server or for the server farm, use Citrix Management Console.

Within the maxmem limit, various combinations of session size and color depth are available. The session size and color depth values are determined using the following formula: height $\times$ width $\times$ depth $\leq$ maxmem, where the height and width are measured in pixels and depth is the color depth in bytes according to the following table:

<table>
<thead>
<tr>
<th>Color depth</th>
<th>Bytes</th>
</tr>
</thead>
<tbody>
<tr>
<td>True Color (24-bit)</td>
<td>3</td>
</tr>
<tr>
<td>High Color (16-bit)</td>
<td>2</td>
</tr>
<tr>
<td>256 Colors</td>
<td>1</td>
</tr>
<tr>
<td>16 Colors</td>
<td>.5</td>
</tr>
</tbody>
</table>

The following is a list of the maximum session sizes with a 4:3 aspect ratio for each color depth at the default maxmem value (height by width by color depth):

- 1600 by 1200 by 24-bit color
- 1920 by 1440 by 16-bit color
- 2752 by 2064 by 256 colors
- 3904 by 2928 by 16 colors

Security Restrictions

None.
This chapter includes information about customizing MetaFrame Setup. Use the information in this chapter to accomplish the following:

- Configure the properties in the MetaFrame Windows Installer installation package with the information needed to create your server farm
- Work with the four sample Windows Installer transform files included on the MetaFrame XP CD
- Create administrative installation packages on network share points so you can install MetaFrame from any location in your network

This chapter describes how to create an administrative installation on a network share point. In the examples in this chapter, the MetaFrame installation package is customized with transforms and placed on a network share point.

**Important** Be sure to read the chapters in this book “Planning for MetaFrame XP Deployment” on page 43 and “Installing MetaFrame XP” on page 105 before you attempt the procedures in this chapter.

The basic procedure for effectively customizing the MetaFrame Windows Installer package is outlined below. Each of these steps is explained in more detail in this chapter. For more information about Windows Installer, including more details about the commands briefly described in this chapter, see the Windows online Help or the Microsoft Web site at http://www.microsoft.com.

### To create customized MetaFrame administrative installation packages

1. Review the sample transform files included on the MetaFrame XP Server CD and gather the information you must enter to transform the installation package.
Note If you are creating a MetaFrame XP server farm with multiple servers, you must modify two transforms; one transform to run on the first server in the farm, and a second transform to run on the servers joining the newly created server farm.

2. Open the MetaFrame installation package in your preferred Windows Installer editing tool and apply a transform. Save the transform with a new name.

Repeat this step for each of the transforms you need to modify. If you are modifying the MetaFrame installation package for two scenarios — creating a farm and joining a farm — you should have two modified transform packages when you are done.

3. Create the network share points for the MetaFrame installation packages. You should create two shares; one for the package transformed to run on the server on which you are creating the server farm, and one for the package transformed to run on the servers joining the server farm.

4. Create the administrative installation packages on the network shares you created in Step 3.

Creating Transforms

You can manipulate the installation process by applying Windows Installer transforms (files with the .mst extension) to the installation database contained in a Windows Installer package. A transform makes changes to elements of the database. A transform file modifies the installation package when it is being installed and dynamically affects the installation behavior.

Transforms that you create to customize a Windows Installer setup package remain cached on your system. These files are applied to the base Windows Installer package whenever the Installer needs to modify it. You can apply transforms only when you initially install Windows Installer packages; you cannot apply transforms to software that is already installed.

When you create a transform to apply to the MetaFrame XP Windows Installer package, you set your desired values for properties in the package. When you then apply the transform to the installation package, the “questions” you would be asked during Setup are answered. Creating a transform allows you to install MetaFrame XP in unattended mode.

There are several commercially available tools you can use to create or edit transforms.
Citrix provides four sample transforms on the MetaFrame XP CD-ROM, located in the Support\Install directory. The transforms include sample values for select properties, allowing you to determine which properties you can edit to achieve a certain configuration.

For definitions and possible values of the properties in the sample transforms, see “MetaFrame Setup Property Names and Values” on page 375.

The transforms in the following examples are used to create a MetaFrame XP server farm using Microsoft Access for the farm’s data store and a server farm using Microsoft SQL Server as the farm’s data store.

**Important**  Do not apply the sample transforms to MetaFrame XP Setup without editing them to include your required values. Some of the commercially available Windows Installer packaging tools allow you to edit existing transforms. Use the sample transforms as a guideline to achieve the desired configuration.

### To create a customized transform using one of the sample transform files

1. Using your preferred tool for editing Windows Installer packages, open the MetaFrame Setup Windows Installer installation package, MFXP001.msi, located on the MetaFrame CD in the \MetaFrame directory.
2. Apply the transform that includes the properties and values you want to modify.
3. Enter new values for the properties you want to change.
4. Generate the transform file and save it with a new name.

### To apply a transform

Type the following at a command prompt where *package* is the name of the MetaFrame XP Windows Installer installation package and *TransformList* is the list of the transforms that you want to apply.

```
msiexec /i package TRANSFORMS=TransformList
```

If you are applying multiple transforms, separate each transform with a semicolon. For further information about the parameters and switches you can use with these options, go to the Microsoft Web site at http://www.microsoft.com and search on “msiexec.”

The properties to set to achieve the results of each sample transform are listed in the following sections.
Create a New MetaFrame XP Server Farm Using a Locally Hosted Data Store (Microsoft Access or MSDE)

This sample transform shows possible values for creating a farm that uses an MSDE database as the server farm’s data store. The database is stored locally on the first server in the farm on which you installed MetaFrame.

The name of the sample transform file on the MetaFrame CD is *Localdb_access_create.mst*.

**Properties and Sample Values**

- `CTX_MF_NEW_FARM_NAME=FarmAccess`
- `CTX_MF_USER_NAME=Administrator`
- `CTX_MF_DOMAIN_NAME=Domain1`
- `CTX_MF_FARM_SELECTION=Create`
- `CTX_MF_CREATE_FARM_DB_CHOICE=Local`
- `CTX_MF_LOCAL_DATABASE=SQL`
- `CTX_MF_MSDE_INSTANCE_NAME=CITRIX_METAFRAME`
- `CTX_MF_NFUSE_DEF_WEB_PAGE=Yes`
- `CTX_MF_SHADOWING_CHOICE=Yes`
- `CTX_MF_XML_PORT_NUMBER=80`
- `CTX_MF_XML_CHOICE=Share`
- `CTX_MF_SERVER_TYPE=a`
- `CTX_MF_PRODUCT_CODE=0A00-0C32`
- `CTX_MF_SHADOW_PROHIBIT_NO_LOGGING=No`
- `CTX_MF_SHADOW_PROHIBIT_NO_NOTIFICATION=No`
- `CTX_MF_SHADOW_PROHIBIT_REMOTE_ICA=No`

These rows are added to the transform because they are not available in the default MetaFrame XP Windows Installer package.

- `CTX_MF_CLIENT_CD_PATH=\fileserver\image`
- `CTX_MF_LAUNCH_CLIENT_CD_WIZARD=Yes`
Join an Existing MetaFrame XP Server Farm that Uses a Locally Hosted Data Store (Microsoft Access or MSDE)

In this sample transform, the existing server farm uses an MSDE database stored on one of the MetaFrame XP servers.

The name of the sample transform file on the MetaFrame CD is **Join_Indirect.mst**.

**Properties and Sample Values**

- `CTX_MF_FARM_SELECTION=Join`
- `CTX_MF INDIRECT_JOIN_USER_NAME=Administrator`
- `CTX_MF INDIRECT_JOIN_DOMAIN_NAME=Domain1`
- `CTX_MF JOIN_FARM_SERVER_NAME=Server1`
- `CTX_MF JOIN_FARM_SERVER_PORT=2512`
- `CTX_MF JOIN_FARM_DB_CHOICE=Indirect`
- `CTX_MF_NFUSE_DEF_WEB_PAGE=Yes`
- `CTX_MF_XML_PORT_NUMBER=80`
- `CTX_MF_XML_CHOICE=share`
- `CTX_MF_SERVER_TYPE=a`
- `CTX_MF_PRODUCT_CODE=0A00-0C32`
- `CTX_MF_SHADOW_PROHIBIT_NO_LOGGING=Yes`
- `CTX_MF_SHADOW_PROHIBIT_NO_NOTIFICATION=No`
- `CTX_MF_SHADOW_PROHIBIT_REMOTE_ICA=No`

These rows are added to the transform because they are not available in the default MetaFrame XP Windows Installer package. If you have a blank password, do not add the password property. In general, if a property exists in the .Msi file and you want to set it to NULL, delete the property in the transform file.

- `CTX_MF_CLIENT_CD_PATH=\fileserver\image`
- `CTX_MF_LAUNCH_CLIENT_CD_WIZARD=Yes`
- `CTX_MF INDIRECT_JOIN_PASSWORD=Password`
Create a New MetaFrame XP Server Farm Using a Data Store on a Separate Database Server (Microsoft SQL, Oracle, or IBM DB2)

This sample transform creates a farm that uses a Microsoft SQL Server, Oracle, or IBM DB2 database as the server farm’s data store. The database is stored on a dedicated database server and is configured for direct access by the servers in the farm.

The name of the sample transform file on the MetaFrame CD is `thirdpartydb_create_direct.mst`.

Properties and Sample Values

```plaintext
CTX_MF_NEW_FARM_NAME=Farm-ThirdParty
CTX_MF_CREATE_FARM_DB_CHOICE=ThirdParty
CTX_MF_USER_NAME=Administrator
CTX_MF_DOMAIN_NAME=Domain1
CTX_MF_FARM_SELECTION=Create
CTX_MF_ODBC_USER_NAME=sa
CTX_MF_ODBC_PASSWORD=citrix
CTX_MF_ODBC_RE_ENTERED_PASSWORD=citrix
CTX_MF_NFUSE_DEF_WEB_PAGE=Yes
CTX_MF_SHADOWING_CHOICE=Yes
CTX_MF_XML_PORT_NUMBER=180
CTX_MF_XML_CHOICE=Separate
CTX_MF_SERVER_TYPE=e
CTX_MF_PRODUCT_CODE=0D00-06A7
CTX_MF_SHADOW_PROHIBIT_NO_LOGGING=No
CTX_MF_SHADOW_PROHIBIT_NO_NOTIFICATION=Yes
CTX_MF_SHADOW_PROHIBIT_REMOTE_ICA=No
```

These rows are added to the transform because they are not available in the default MetaFrame XP Windows Installer package.

```plaintext
CTX_MF_CLIENT_CD_PATH=\fileserver\image
CTX_MF_LAUNCH_CLIENT_CD_WIZARD=Yes
CTX_MF_SILENT_DSNFILE =\fileserver\image\TestSQL.DSN
```
Join an Existing MetaFrame XP Server Farm that Uses a Data Store on a Separate Database Server (Microsoft SQL, Oracle, or IBM DB2)

In this sample transform, the existing server farm uses a SQL, Oracle, or IBM DB2 database stored on a dedicated database server. The new server joining the farm accesses the data store directly.

The name of the sample transform file on the MetaFrame CD is thirdpartydb_join_direct.mst.

Properties and Sample Values

- CTX_MF_FARM_SELECTION=Join
- CTX_MF_JOIN_FARM_DB_CHOICE=Direct
- CTX_MF_ODBC_USER_NAME=sa
- CTX_MF_ODBC_PASSWORD=citrix
- CTX_MF_ODBC_RE_ENTERED_PASSWORD=citrix
- CTX_MF_NFUSE_DEF_WEB_PAGE=Yes
- CTX_MF_SHADOWING_CHOICE=Yes
- CTX_MF_XML_PORT_NUMBER=180
- CTX_MF_XML_CHOICE=Separate
- CTX_MF_SERVER_TYPE=e
- CTX_MF_PRODUCT_CODE=0D00-06A7
- CTX_MF_SHADOW_PROHIBIT_NO_LOGGING=No
- CTX_MF_SHADOW_PROHIBIT_NO_NOTIFICATION=Yes
- CTX_MF_SHADOW_PROHIBIT_REMOTE_ICA=No

These rows are added to the transform because they are not available in the default MetaFrame XP Windows Installer package.

- CTX_MF_CLIENT_CD_PATH=\fileserver\image
- CTX_MF_LAUNCH_CLIENT_CD_WIZARD=Yes
- CTX_MF_SILENT_DSNFILE =\fileserver\image\TestSQL.DSN
Creating Administrative Installations

You can use Windows Installer to perform an administrative installation of MetaFrame. An administrative installation decompresses the installation files and copies them to a network share point. You can create customized images of MetaFrame Setup on share points. Users who can access the share point can then run MetaFrame Setup from the source image.

When you create and maintain an administrative source image, you can apply any Windows Installer patch files (files with the .msp extension) to the image as they are released. Applying patch files to the source image allows you to install the patches when you install the application on a clean system; you do not have to install the patches separately after you install the application.

You create administrative installations on network share points only once. Citrix recommends that you create the following two administrative installation source images:

- The MetaFrame installation package and any transforms needed to create the server farm. Run this image on the first server in the server farm.
- The MetaFrame installation package and any transforms needed to join other servers to the server farm. Run this image on all servers joining an existing server farm.

Follow the steps below to create an administrative installation on a network share point.

To create an administrative installation

1. Copy the MetaFrame XP server CD image to a network location so that you can refer back to it if necessary.
2. Create the appropriate transform files to create a new server farm and to join a server farm.
3. Run the msiexec /a command to create two network images from which MetaFrame XP can be installed:
   - The image to use when creating a server farm
   - The image to use when joining a server farm

The following is an example of the command line to use to accomplish this:

```plaintext
msiexec /a <full path the base mfxp001.msi package> /L*v <full path to a log file> /qb TARGETDIR="<full path to the network location>"
TRANSFORMS=<(semi-colon delimited list of the appropriate transform file(s) created from Step 2 (example: sql_join.mst))>
```
4. Run MetaFrame XP Setup from the network share points you created. Start with the share point that contains the image used to create the first server in the farm. The following is an example of a command line to accomplish this:

```
msiexec /i <full path to my new share point mfxp001.msi> /L <full path to a log file location> /qb-
```

**MetaFrame Setup Property Names and Values**

Some values, such as passwords, may be case-sensitive. Values that include spaces must be enclosed in quotation marks (""") if you are using them in a command line.

**CTX_MF_USER_NAME**

Definition: User name for the initial MetaFrame XP administrator credentials; applies only when creating a farm.

Possible values: User defined

Default value: “UserName”

**CTX_MF_DOMAIN_NAME**

Definition: Domain name for the farm administrator credentials; applies only when creating a farm.

Possible values: User defined

Default value: “DomainName”

**CTX_MF_SHADOWING_CHOICE**

Definition: Turn ICA session shadowing on or off.

**Important** If you turn session shadowing off when you install MetaFrame, you cannot enable shadowing at a later time through user policies or connection configuration.

Possible values: “Yes” - turn it on, or “No” - turn it off

Default value: “Yes”

**CTX_MF_SHADOW_PROHIBIT_REMOTE_ICA**

Definition: Prohibit or do not prohibit remote control of mouse and keystrokes in ICA sessions.

Possible values: “Yes” - Prohibit, or “No” - Do not prohibit

Default value: “No”
**CTX_MF_SHADOW_PROHIBIT_NO_NOTIFICATION**

Definition: Prohibit or do not prohibit shadowing connections without user notification.

Possible values: “Yes” - Prohibit, or “No” - Do not prohibit

Default value: “No”

**CTX_MF_SHADOW_PROHIBIT_NO_LOGGING**

Definition: Prohibit or do not prohibit shadow connections without logging.

Possible values: “Yes” - Prohibit, or “No” - Do not prohibit

Default value: “No”

**CTX_MF_FARM_SELECTION**

Definition: Defines whether you are creating a new MetaFrame server farm or joining an existing MetaFrame server farm.

Possible values: “Create” - create a farm, or “Join” - join a farm. If this server is joining an existing farm, you must set the CTX_MF_JOIN_FARM_DB_CHOICE property.

Default value: “Create”

**CTX_MF_CREATE_REMOTE_DESKTOP_USERS**

Definition: Determines whether or not to add users to the Remote Desktop Users group on a Windows Server 2003 server. Users must be members of the Remote Desktop Users group to log in remotely to a Windows Server 2003 server.

Setting this property has no effect if the server is running Windows 2000, or if the Remote Desktop Users group already has members.

Possible values:

“AddEveryone” — Adds the Authenticated Users group to the Remote Desktop Users group. This option allows all current and future authenticated users to log on remotely to the server.

“CopyUsers” — Copies all current users from the Users group to the Remote Desktop Users group. Any user accounts you add must be added to the Remote Desktop Users group manually.

“DoNothing” — Does not add any users to the Remote Desktop Users group. Choosing this option means that no users will be allowed to log on remotely to the server until you add users to the Remote Desktop Users group in Windows Server 2003.

Default value: “CopyUsers”.
**CTX_ENABLE_DOWNGRADE**

Definition: Creates a backup copy of the files that are currently on your system. Files are backed up under [INSTALLDIR]DowngradeBackup\ (Usually C:\Program Files\Citrix\DowngradeBackup\).

Possible values: Yes, No

Default value: Yes

**CTX_MF_INITLICENSEDB**

Definition: Communicates MetaFrame XP license information to the farm’s data store.

Possible values: Yes - Initialize the data store to communicate MetaFrame XP feature release license information; No - Do not initialize the data store to communicate feature release license information. Enter “No” if the data store was already updated by one of the servers in the farm.

Default value: Yes

Best practices: Use the default value if you are creating a new MetaFrame XP server farm on the first server on which you are running MetaFrame XP Setup. If you are joining additional servers to the newly created farm, set CTX_MF_INITLICENSEDB to “No.”

If you are upgrading a MetaFrame XP server farm to the latest MetaFrame XP feature release, use the default value for CTX_MF_INITLICENSEDB for the first server you upgrade and then set CTX_MF_INITLICENSEDB to “No” for all additional servers you are upgrading.

**CTX_MF_NFUSE_DEF_WEB_PAGE**

Definition: Changes the server’s default Web page to the Web Interface for MetaFrame XP logon page; used only if also installing the Web Interface on the MetaFrame server.

Possible values: “Yes” or “No”

Default value: “Yes”
**CTX_MF_XML_CHOICE**
Definition: Determines whether Microsoft Internet Information Services (IIS) and the Citrix XML Service share the same port on this MetaFrame server or use separate ports. If you do not want IIS and the XML Service to share the same port, you must set the XML Service port number in CTX_MF_XML_PORT_NUMBER.
Possible values: “Share” - share with IIS, or “Separate” - use separate port, set in CTX_MF_XML_PORT_NUMBER.
Default value: “Share”

**CTX_MF_XML_PORT_NUMBER**
Definition: Port number you want the Citrix XML Service to use when you do not want the XML Service and IIS to share ports.
Possible values: User defined
Default value: “80”

**CTX_MF_CREATE_FARM_DB_CHOICE**
Definition: When creating a new farm, specify whether the database is a local database (Access or MSDE) stored on the first server in the new farm, or a third-party database stored on a separate database server (SQL, Oracle, or IBM DB2).
Possible values: “ThirdParty” or “Local”
Default value: “Local”

**CTX_MF_LOCAL_DATABASE**
Definition: Type of locally stored database that stores the MetaFrame farm’s data store.
Possible values: “Access” or “SQL” (SQL for MSDE)
Default value: “Access”

**CTX_MF_MSDE_INSTANCE_NAME**
Definition: If using MSDE for a local database, you can specify an installed instance of MSDE instead of using the default. If you specified an instance of MSDE other than the default — for example, if you installed MSDE using a command prompt and specified custom options — you must enter the name of the custom instance you installed.
Possible values: User defined.
Default value: CITRIX_METAFRAME.
**CTX_MF_ODBC_PASSWORD**

Definition: Password for the third-party database that stores the MetaFrame farm’s data store.

Possible values: User defined

Default value: “Password”

**CTX_MF_ODBC_USER_NAME**

Definition: User name for a third-party database that stores the MetaFrame farm’s data store.

Possible values: User defined.

Default value: “UserName”

**CTX_MF_SILENT_DSNFILE**

Definition: Path to the DSN file to be used for the data store - use for silent installation.

Possible values: Complete path to the DSN file

Default value: “” (null)

**CTX_MF_JOIN_FARM_DB_CHOICE**

Definition: Use when joining this server to an existing MetaFrame server farm.

Possible values: “Direct” or “Indirect.”

Set this property’s value to “indirect” if you are using a Microsoft Access or MSDE database, stored locally on the first server in the farm on which you installed MetaFrame, for the data store. Set this property’s value to “direct” if you are using a Microsoft SQL, Oracle, or IBM DB2 database, stored on a separate dedicated database server, for the data store.

Default value: “Direct”

**CTX_MF_INDIRECT_JOIN_DOMAIN_NAME**

Definition: Domain name of a user account that has full administration rights in MetaFrame. Define if you are joining a farm that uses a Microsoft Access or MSDE database, stored locally on the first server in the farm, for the data store (indirect access).

Possible values: Can be any user’s domain (the user account must have full administration rights in MetaFrame).

Default value: “DomainName”
**CTX_MF_NEW_FARM_NAME**

Definition: The name of the new farm; always specify if you are creating a new farm.

Possible values: User defined.

Default value: “NewFarmName”

**CTX_MF_INDIRECT_JOIN_USER_NAME**

Definition: User name of a user account that has full administration rights in MetaFrame. Define if you are joining a farm that uses a Microsoft Access or MSDE database, stored locally on the first server in the farm, for the data store (indirect access).

Possible values: Can be any user who has full administrative privileges in MetaFrame.

Default value: “Administrator”

**CTX_MF_INDIRECT_JOIN_PASSWORD**

Definition: The password for a user account that has full administration rights in MetaFrame. Define if you are joining a farm that uses a Microsoft Access or MSDE database, stored locally on the first server in the farm, for the data store (indirect access).

Possible values: The password for the user name entered in CTX_MF_INDIRECT_JOIN_USER_NAME.

Default value: “” (null)

**CTX_MF_JOIN_FARM_SERVER_NAME**

Definition: Name of a MetaFrame XP server in the farm you want to join.

Possible values: Any server in the MetaFrame XP server farm.

Default value: “ServerName”

**CTX_MF_JOIN_FARM_SERVER_PORT**

Definition: Port number for the IMA communication port used to communicate with the locally stored server farm data store (for example, if you are using a Microsoft Access or MSDE database, stored locally on the first server in the farm on which you installed MetaFrame, for the data store).

Possible values: User defined

Default value: “2512”
REBOOT
Definition: Standard Windows Installer property that controls whether you restart a server or prompt for the server to be restarted
Possible values: “Force” - Forces reboot to occur, no further prompts are displayed.
“Suppress” - Forces reboot to not occur by default; a prompt occurs if action is necessary.
“ReallySuppress” - Force reboot to not occur, no prompts appear.
Default value: “Force”

CTX_MF_ZONE_NAME
Definition: Name of the zone to which the server belongs.
Possible values: Not applicable
Default value: None. The default value for the zone name is generated programatically, based on the subnet address of the server.

CTX_MF_LAUNCH_CLIENT_CD_WIZARD
Definition: Specifies whether or not to launch the ICA Client Distribution wizard (to update the ICA Clients images on the MetaFrame server).
Possible values: “Yes”- Launch wizard, or “No” - Do not launch wizard; that is, do not update client images.
Default value: “No”

CTX_MF_CLIENT_CD_PATH
Definition: Path to the MetaFrame XP Components CD-ROM; to be passed to the ICA Client Distribution wizard.
Possible values: Complete path to the Components CD-ROM.
Default value: “” (null)

CTX_MF_PRODUCT_CODE
Definition: Product code of the MetaFrame server you are trying to install. If you are performing a silent installation and using a command line, the command line arguments for this property must be set to the correct value.
Possible values: The product code on the MetaFrame XP CD-ROM.
Default value: “0D00-06A7” (the product code for the MetaFrame XPe product type)
CTX_MF_SERVER_TYPE
Definition: The family level of MetaFrame to be installed. If you are performing a silent installation and using a command line, the command line arguments for this property must be set to the correct value.
Possible values: “E” for MetaFrame XPe, “A” for MetaFrame XPa, or “S” for MetaFrame XPs.
Default value: “E”

INSTALLDIR
Definition: The target location for the MetaFrame installation.
Possible values: User defined.
Default value: %Program Files%\Citrix
**CTX_ADDLOCAL**

Definition: This property is similar to the Windows Installer ADDLOCAL property.

Possible values: Blank (default), All, CTX_MF_MetaFrame_Core, CTX_MF_IM, CTX_MF_IM_Packager, CTX_MF_IM_Service, CTX_MF_LM, CTX_MF_NFuse, CTX_MF_NM, CTX_MF_RM, PN_ENGINE, PN, PN_AGENT, WMI, MetaFrame_XP, CTX_MF_CMC, CTX_MF_ICA_Shell_Editor, CTX_MF_IMA_Core, CTX_MF_IM_Plugin, CTX_MF_RM_Plugin.

Separate entries by commas. Valid configurations are:

- **All** — Install every feature (XPE configuration).
- **MetaFrame_XP,CTX_MF_MetaFrame_Core,CTX_MF_IMA_Core,CTX_MF_ICA_Shell_Editor** — Core MetaFrame, required for any configuration (referred to below as @Core).
- **PN, PN_ENGINE** — Install the full Program Neighborhood client as the Pass-Through Client (referred to below as @PN).
- **PN_AGENT, PN_ENGINE** — Install the Program Neighborhood Agent as the Pass-Through Client.
- **CTX_MF_NFuse** — Install the Web Interface for MetaFrame XP on the MetaFrame XP server.
- **CTX_MF_CMC,CTX_MF_IM_Plugin,CTX_MF_RM_Plugin** — Install the Management Console for MetaFrame XP (referred to below as @CMC).
- **CTX_MF_IM_Service** — Install the Installation Manager installer service.
- **CTX_MF_IM_Packager** — Install the Installation Manager Packager
- **CTX_MF_IM,CTX_MF_IM_Service,CTX_MF_IM_Packager** — Install all Installation Manager components (referred to below as @IM).
- **CTX_MF_RM** — Install Resource Manager
- **@Core,CTX_MF_LM,WMI,@CMC,CTX_MF_NFuse,PN,@IM,CTX_MF_RM** — Install all default MetaFrame XPe components.
- **@Core,CTX_MF_LM,@CMC,CTX_MF_NFuse,PN** — Install all default MetaFrame XPa components.
- **@Core,@CMC,CTX_MF_NFuse,PN** — Install all default MetaFrame XPs components.

Default value: Blank
REINSTALLMODE

Definition: Specifies the type of reinstall to perform. Options are case-insensitive and order-independent.

Possible values:
- p - install missing files
- o - replace older versioned or missing files
- c - replace corrupt files (checksum validation)
- e - replace same versioned or missing files
- d - replace files of differing versions
- a - replace all files regardless of version
- u - replace user registry settings
- m - replace machine registry settings
- s - replace shortcuts
- v - replace the cached MSI package with the package we are installing from

Default value: oums

**Important** Citrix recommends that you do not modify this property.
CTX_MF_ENABLE_VIRTUAL_SCRIPTS
Definition: Directs MetaFrame XP Setup to create the virtual scripts directory. If the value is set to “Yes” or “1”, Setup does not display the dialog box asking for permission to create the virtual scripts directory, even if you are running Setup in full UI mode.

If you are running a “silent” installation where this property is not set to “Yes” or “1” and the XML port on the MetaFrame XP server is shared with IIS (if you are installing the Web Interface, for example), Setup aborts and the following error message is added to the installation log file:

“ERROR: SetIISScriptsDir - Could not get the scripts path because the Virtual Scripts directory in not enabled in IIS or the property CTX_MF_ENABLE_VIRTUAL_SCRIPTS is not set to Yes."

If the property is defined, the silent installation continues with no error.
Possible Values: “Yes” or “1” - Create the virtual scripts directory if it doesn't already exist.
Not defined, “0”, or “No” - Do not create the virtual scripts directory if it doesn't already exist. You are prompted during Setup to create the virtual scripts directory.

Default Value: Not defined

CTX_MF_ADD_LOCAL_ADMIN
Definition: If enabled, creates MetaFrame XP administrator accounts for all user accounts in the local Administrators group.
Possible values: “Yes” “No”.
Default value: “No”

Pass-Through Client Properties
Use the following properties if you are installing the Pass-Through Client.

CLIENT_INSTALLDIR
Definition: The target location for the Pass-Through Client installation.
Possible values: User defined.
Default value: %Program Files%\Citrix\ICA Client
ENABLE_DYNAMIC_CLIENT_NAME

Definition: When using the ICA Pass-Through Client, turn on or off the capability to use the computer name as the client device name and recognize changes to the client name.

Possible values: “Yes” “No”.
Default value: “Yes”

PROGRAM_FOLDER_NAME

Definition: \(<\text{Start Menu Program Folder Name}>\), where \(<\text{Start Menu Program Folder Name}>\) is the name of the Programs folder on the Start menu containing the shortcut to the Program Neighborhood or Program Neighborhood Agent software.

Possible values: User defined.
Default value: If installing the full Program Neighborhood Client, the default value is “Citrix ICA Client.” If installing the Program Neighborhood Agent, the default is “Citrix Program Neighborhood Agent.”

SERVER_LOCATION

Definition: The URL of the server running the Web Interface for MetaFrame XP. This server hosts the configuration file for the Program Neighborhood Agent. You must enter the server address if you want to use the Program Neighborhood Agent as the Pass-Through Client on this MetaFrame XP server. The server address can use HTTP or HTTPS.

Possible values: User defined
Default value: localhost

DEFAULT_NDSCONTEXT

Definition: Include this parameter if you want to set a default context for NDS. If you are including more than one context, place the entire value in quotation marks, and separate the contexts by a comma.

Examples of correct parameters:
DEFINL_NTSCONTEXT=Context1
DEFAULT_NDSCONTEXT="Context1,Context2"

Example of an incorrect parameter:
DEFAULT_NDSCONTEXT=Context1,Context2
ENABLE_SSON

Definition: Set to Yes to enable Single Sign-On (Pass-Through Authentication) for the pass-through client. Set to No to disable Single Sign-On for the pass-through client.

Default value: “Yes”
Glossary

account authority  The platform-specific source of information about user accounts used by a MetaFrame XP server, for example, a Windows NT domain, Active Directory domain, or Novell Directory Services (NDS).

activation code  An alphanumeric string displayed on the Citrix Activation System Web page after you enter a license number. To activate a license, select the license number in the Management Console for MetaFrame XP and enter the activation code.

anonymous application  An application published exclusively for the use of anonymous users.

anonymous session  An ICA session started by an anonymous user.

anonymous user  An unidentified user granted minimal access to a MetaFrame XP server, or server farm, and its published applications.

anonymous user account  A user account defined on a MetaFrame XP server for access by anonymous users.

application name  A text string used to uniquely identify a published application within a farm. The application name is used by the MetaFrame XP server farm and ICA Clients to recognize individual applications that may have the same display name. The text string is automatically generated based on the display name entered when the application was initially published.

Application Launching and Embedding (ALE)  A feature of MetaFrame XP servers and ICA Clients that enables full-function, Windows-based applications to be launched from or embedded into HTML pages without rewriting any application code.

application set  A user’s view of the applications published on a server farm that the user is authorized to access.

automatic client update  The MetaFrame XP server feature that enables you to install the latest versions of ICA Clients on your servers, then schedule the download and installation of that software to your users’ client devices.
automatic client reconnect  The feature that prompts supported ICA Clients to automatically reconnect to a session when dropped connections are detected (when network issues outside of MetaFrame XP occur).

certificate store  The location on the MetaFrame XP server running the SSL Relay that contains the server certificate. The certificate for the SSL Relay should be in Local computer/Personal so that you can manage it with the Certificate snap-in for Microsoft Management Console.

ciphersuite  An encryption/decryption algorithm. When establishing an SSL connection, the client and server determine a common set of supported ciphersuites and then use the most secure one to encrypt the communications. Ciphersuites have different advantages in terms of speed, encryption strength, exportability, and so on.

Citrix Program Neighborhood Agent  The Citrix Program Neighborhood Agent allows you to deliver published applications directly to users' desktops so users can access links to published applications with or without a Web browser. With the Program Neighborhood Agent, links to published applications appear in the Start menu, on the Windows desktop, or in the Windows System Tray. Remote applications are integrated into the desktop and appear to the user as local applications. You must use the Web Interface for MetaFrame XP to use the Program Neighborhood Agent.

Citrix Program Neighborhood Agent Admin tool  Use the Citrix Program Neighborhood Agent Admin tool to centrally configure user settings that are pushed out to all users running the Program Neighborhood Agent.

Citrix SSL Relay  A Windows service that runs on a MetaFrame XP server to support an SSL-secured connection between a server running the Web Interface for MetaFrame XP and a server running MetaFrame XP Server. See also “Secure Sockets Layer (SSL)/Transport Layer Security (TLS)” on page 396 and “ICA Encryption” on page 393.

Citrix XML Service  A Windows service that provides an HTTP interface to the ICA Browser. It uses TCP packets instead of UDP, which allows connections to work across most firewalls. The default port for the Citrix XML Service is 80.

client COM port mapping  The feature that enables applications running on a MetaFrame XP server to access peripherals attached to COM ports on the client device.

client device  Any hardware device capable of running the ICA Client software.

client device mapping  The feature that enables remote applications running on the MetaFrame XP server to access storage and peripherals attached to the local client device. Client device mapping consists of several distinct features: client drive mapping, client printer mapping, and client COM port mapping.

client drive mapping  The feature that enables applications running on the MetaFrame XP server to access physical and logical drives configured on the client device.

client printer mapping  The feature that enables applications running on the MetaFrame XP server to send output to printers configured on the client device.
client update database  The database MetaFrame XP servers use to automatically update ICA Clients. It contains copies of the clients themselves and configuration information about how to perform the updates.

collection control  The feature that allows you to set a limit on the number of connections that each user can have simultaneously in the server farm. You can also limit the number of concurrent connections to specified published applications, and you can prevent users from launching more than one instance of the same published application.

collection license  A license that enables ICA connections between a client device and a MetaFrame XP server farm. Connection license counts can be assigned to specific servers; they are automatically pooled among all servers in the farm.

content publishing  This feature allows you to publish document files, media files, Web URLs, and any other type of file from any network location. Icons for published content appear in Program Neighborhood, on the desktop, and on the user’s Web Interface logon page. Users can double-click published content icons to access content in the same way they access published applications.

Content Redirection  This feature allows administrators to specify whether ICA Clients open published content, applications, browsers, and media players locally or remotely. There are two types of content redirection: from server to client and from client to server.

custom ICA connection  A user-created shortcut to a published application or MetaFrame XP server.

CPU prioritization  The feature that allows you to assign each published application in the server farm a priority level for CPU access. This feature can be used to ensure that CPU-intensive applications in the server farm do not degrade the performance of other applications.

data collector  A MetaFrame XP server that stores dynamic data for one zone in a MetaFrame XP server farm.

data store  An ODBC-compliant database used by a MetaFrame XP server farm. The data store centralizes configuration information about published applications, users, printers, and servers. Each MetaFrame XP server farm has a single data store.

delegated administration  The feature that allows you to delegate areas of MetaFrame XP administration and farm management to your IT staff. Administrators can assign specialized staff members to perform specific MetaFrame XP tasks such as managing printers, published applications, or user policies. Specialized staff members can carry out their assigned tasks without being granted full access to all areas of farm management.
**disconnected session**  An ICA session in which the ICA Client is no longer connected to the MetaFrame XP server, but the user’s applications are still running. A user can reconnect to a disconnected session. If the user does not do so within a specified time-out period, the MetaFrame XP server automatically terminates the session.

**display name**  A name you specify when you publish an application. The display name appears in the newer Program Neighborhood client and in Application folders in the Management Console for MetaFrame XP. You can also choose to use the display name in the Web Interface for MetaFrame XP.

**dynamic store**  A data store that contains frequently updated configuration data such as application load and license usage information. A server farm replicates dynamic store information across multiple servers.

**file type association**  You configure content redirection from client to server by associating published applications with file types and then assigning them to the users you want to be affected.

**ICA**  Independent Computing Architecture. The architecture that Citrix uses to separate an application’s logic from its user interface. With ICA, only the keystrokes, mouse clicks, and screen updates pass between the client and server on the network, while 100% of the application’s logic executes on the server.

**ICA asynchronous connections**  Asynchronous connection types allow direct dial-in to a MetaFrame XP server without the overhead of RAS and TCP/IP.

**ICA Browser**  See master ICA Browser or master browser.

**ICA Client**  Citrix software that enables users to connect to MetaFrame XP servers from a variety of client devices.

**ICA Client Creator**  The MetaFrame XP server utility you use to create disks from which you can install ICA Clients and the ICA File Editor on a wide range of client devices.

**ICA Client Printer Configuration**  The utility you use to create and connect to client printers for ICA DOS and WinCE Clients. You must run this utility in an ICA session from the client whose printer you want to configure.

**ICA Client Update Configuration**  The utility you use to configure the client update database.

**ICA connection**  The logical port used by an ICA Client to connect to, and start a session on, a MetaFrame XP server. 1. An ICA connection is associated with a network connection (such as TCP/IP, IPX, SPX, or NetBIOS) or a serial connection (modems or direct cables). 2. The active link established between an ICA Client and a MetaFrame XP server.
ICA Encryption This feature enables use of the SSL (Secure Sockets Layer) or TLS (Transport Layer Security) protocols to secure communication between the ICA Clients that support SSL and MetaFrame XP servers. SSL provides server authentication, encryption of the data stream, and message integrity checks. After configuring the Citrix SSL Relay, you can specify the use of SSL when you publish applications. See also Citrix SSL Relay.

ICA file A text file (with the extension ica) containing information about a published application. ICA files are written in Windows Ini file format and organize published application information in a standard way that ICA Clients can interpret. When an ICA Client receives an ICA file, it initializes a session running the specified application on the MetaFrame XP server specified in the file.

ICA protocol The protocol that ICA Clients use to format user input (keystrokes, mouse clicks, and so forth) and address it to MetaFrame XP servers for processing. MetaFrame XP servers use it to format application output (display, audio, and so forth) and return it to the client device.

ICA session A lasting connection between an ICA Client and a MetaFrame XP server, identified by a specific user ID and ICA connection. It consists of the status of the connection, the server resources allocated to the user for the duration of the session, and any applications executing during the session. An ICA session normally terminates when the ICA Client user logs off the MetaFrame XP server.

Independent Management Architecture (IMA) Citrix’s server-to-server infrastructure that provides robust, secure, and scalable tools for managing any size server farm. Among other features, IMA enables centralized platform-independent management, an ODBC-compliant data store, and a suite of management products that plug in to the Management Console.

interoperability The MetaFrame XP ability to work in mixed mode with MetaFrame 1.8 servers in the same server farm. Not all MetaFrame XP features are available in mixed mode.

key store The directory on the MetaFrameXP server running the SSL relay that contains the server certificate. The default directory is %SystemRoot%\SSLRelay\keystore\certs.

license count The number of server installations or ICA connections that a MetaFrame XP license authorizes.

license number An alphanumeric string displayed by the Management Console when you enter a license serial number. You enter the resulting license number on the Citrix Activation System Web page to receive an activation code for the license.

license pooling A feature of MetaFrame XP servers that enables you to combine license counts of product and connection licenses into a common license pool for a server farm. All license counts are pooled by default. Assigning a license count to a server removes it from the pool.
load management  A feature of MetaFrame XPA and MetaFrame XPe that enables management of application loads. When a user launches a published application that is configured for load management, that user’s ICA session is established on the most lightly loaded server in the farm, based on criteria you can configure.

local text echo  A feature that accelerates the display of text input on a client device to effectively shield users from experiencing latency on the network.

Management Console for MetaFrame XP  The extensible, platform-independent tool for administering MetaFrame XP servers and management products.

master ICA Browser or master browser  The ICA Browser on one MetaFrame XP server in a network that gathers information about licenses, published applications, performance, and server load from the other member browsers within the network and maintains that information.

member ICA Browser or member browser  The ICA Browsers on the MetaFrame XP servers in a network that forward information about licenses, published applications, performance, and server load to the master browser.

MetaFrame XP administrators  System administrators responsible for installing, configuring, and maintaining MetaFrame XP servers. In a UNIX environment, it is the user group assigned to these administrators, which has the default name ctxadm.

MetaFrame XP servers  Servers on which Citrix MetaFrame XP software is running. You can publish applications, content, and desktops for remote access by ICA Clients on these servers.

mixed mode  The mode in which MetaFrame XP servers operate when a server farm contains both MetaFrame XP servers and MetaFrame 1.8 servers. See also interoperability.

mouse-click feedback  A feature that enables visual feedback for mouse clicks. When a user clicks the mouse, the ICA Client software immediately changes the mouse pointer to an hourglass to show that the user’s input is being processed.

native mode  The mode in which MetaFrame XP servers operate when only IMA-based MetaFrame XP servers exist in the network and the option to work with MetaFrame 1.8 servers in the network is not selected. See also interoperability.

NDS support  Support for Novell Directory Services allows users in Novell network environments to log on using their NDS credentials to access applications and content published in MetaFrame XP server farms.

neighborhood folder  A group of logically related applications within a user’s application set. You can assign an application to a specific neighborhood folder when you publish it.

network printer  A printer that is connected to a network print server.
panning and scaling  ICA Client features users can use to view a remote session that is larger than the client desktop. For example, if the client desktop is 1024 x 768 and the ICA session is 1600 x 1200 pixels, the session image does not fit in the session view window. Panning provides scroll bars. Scaling provides controls in the System menu to shrink the session window.

Pass-Through Authentication  When you enable pass-through authentication for the Management Console for MetaFrame XP, the console uses your local user credentials from the server on which the console is running. You can log on without re-entering credentials. Users can also enable Pass-Through Authentication in ICA Clients that support this feature.

pass-through client  An ICA Client installed on a MetaFrame XP server so that users of every ICA Client platform can access published applications by connecting to them through Program Neighborhood as a published application.

policies  Policies are used to apply MetaFrame XP settings, for client device mapping, for example, to specific users or user groups. They override similar MetaFrame XP settings configured farm-wide, at the server level, or on the ICA Client.

product code  A nine-character string that identifies a MetaFrame XP server product. A server farm can contain MetaFrame XP servers with different versions of the same core product; for example, full retail, evaluation, and not-for-resale versions of MetaFrame XP. The product code allows a MetaFrame XP server to locate its product license among the product licenses stored for the entire server farm.

product license  A software license that enables a MetaFrame product.

Program Neighborhood  The user interface for the ICA Win32 Program Neighborhood Client, which lets users view the published applications they are authorized to use in the server farm. Program Neighborhood allows access to application sets and custom ICA connections.

published application  An application installed on a MetaFrame XP server or server farm that is configured for multiuser access from ICA Clients. With Load Manager, you can manage the load for published applications among servers in the server farm. With Program Neighborhood and the Web Interface for MetaFrame XP, you can push a published application to your users’ client desktops.

published content  A document, media clip, graphic, or other type of file or URL that you publish for access by ICA Client users. Published content is executed by local applications on client devices.

relay listening port  The TCP port on the MetaFrame XP server that the Citrix SSL Relay monitors for data from a Web server.
remote node  A client device that can connect to a LAN or WAN with a modem and additional software, such as Microsoft’s Dial-Up Networking. When connected, the device has access to the same network resources as any other node in the network, but is still subject to bandwidth limitations and modem performance.

seamless window  One of the settings you can specify for the Window Size property of a published application. If a published application runs in a seamless window, the user can take advantage of all the client platform’s window management features, such as resizing, minimizing, and so forth.

Secure Sockets Layer (SSL)/Transport Layer Security (TLS)  A standards-based architecture for encryption, authentication, and message integrity. It is used to secure the communications between two computers across a public network, authenticate the two computers to each other based on a separate trusted authority, and ensure that the communications are not tampered with. SSL/ TLS supports a wide range of ciphersuites.

serial number  An alphanumeric string that you enter in the Management Console to receive a license number for the software installed on a server.

server farm  A group of MetaFrame XP servers managed as a single entity, with some form of physical connection between servers and a database used for the farm’s data store.

server-based computing  Citrix’s model for computing where applications are published on centralized servers, or server farms, and users access and run those applications from remote client devices. Server-based computing differs from traditional client-server computing in that all the application logic executes on the host, consuming less network bandwidth and requiring far fewer client resources.

session ID  A unique identifier for a specific ICA session on a specific MetaFrame XP server.

Shadow Taskbar  The taskbar on a MetaFrame XP server desktop that you can use to shadow multiple users and to quickly switch between shadowed sessions.

shadowing  A feature of MetaFrame XP servers that enables an authorized user to remotely join or take control of another user’s ICA session for diagnosis, training, or technical support. See also user-to-user shadowing.

SOCKS  SOCKS is a protocol for secured TCP communications through a proxy server.

SpeedScreen Browser Acceleration  The feature that provides substantial performance enhancements for users running HTML-capable applications, such as Internet Explorer, published on MetaFrame XP servers. SpeedScreen Browser Acceleration requires less bandwidth and allows users running ported applications to interact with the browser while graphically-rich pages or large images are being downloaded.
**SpeedScreen Latency Reduction**  A combination of technologies implemented in ICA that decreases bandwidth consumption and total packets transmitted, resulting in reduced latency and consistent performance regardless of network connection.

**universal printing**  When you use MetaFrame XP Universal Printing you do not need to install and duplicate a potentially large set of native printer drivers in your server farm. The universal printer drivers can replace multiple native printer drivers that would otherwise be needed in diverse printing environments. Later ICA clients can work with universal drivers depending on the client device’s version and platform.

**User-to-User Shadowing**  The feature that allows users to shadow other users without requiring administrator rights. Multiple users from different locations can view presentations and training sessions, allowing one-to-many, many-to-one, and many-to-many online collaboration. See also shadowing.

**Web-based ICA Client installation**  A Web-based method for deploying ICA Client software to users. You construct an ICA Client download Web site that users access to download the ICA Client for their client devices.

**Windows-Based Terminal (WBT)**  A fixed-function thin-client device that can run applications only by connecting to a MetaFrame XP application server. WBTs cannot run applications locally.

**zone**  A logical grouping of MetaFrame XP servers, typically related to the underlying network subnets. All MetaFrame XP servers in a zone communicate with the MetaFrame XP server designated as the data collector for the zone.
Index

A

Acrcfg command 313
Acrobat Reader program 15
activation codes 138, 146, 148
Active Directory Services 66
Address List for client browsing 84
administration tools
   see management tools
administrator accounts
   see MetaFrame XP administrators
ALE 254
Altaddr command 316
anonymous applications and users 248
anonymous users 248
App command 318
applications
   associating with file types 250
data about 271
launching and embedding 254
passing parameters to published applications 253
publishing 244, 249
   see publishing applications
redirecting launching 255
setting CPU priority for 261
Apputil command 321
assigning licenses to servers 151
Async Test dialog box 205
asynchronous connection options 204–206
asynchronous ICA connections 46, 198
audio mapping 217
Auditlog command 324
authentication, user 69, 71–72, 77–78, 105, 119, 237, 245, 277, 281
Auto Client Reconnect feature 276
automatic client update 227

B

bandwidth and compression counters 288
broadcasts
   MetaFrame XP server response to 84
   UDP 184
BUILTIN group 76

C

Change Client command 326
Chfarm command 330
Citrix Activation System 149
Citrix Connection Configuration 195–196, 198–202, 204–206
Citrix Documentation Library 18
Citrix SSL Relay 38, 159, 162, 166
   changing the port 166
Citrix Web Console 39, 170, 181, 273
Citrix Web site 17
Citrix XML Service 85, 125, 337
Clicense command 333
client device mapping 214
client printers 291
Client Update Configuration utility 229
Client Update Database 229–236, 240
   adding clients 233
   changing client properties 235
   configuring update options 231
   creating a new database 230
   removing clients 235
   specifying a default database 230
cloning MetaFrame XP servers 133
Cltprint command 336
COM port mapping 217
commands 311–366
configuring
   anonymous user accounts 249
   Citrix SSL Relay 162
   client device mapping 213
   client reconnection settings 278
   Connection Control settings 268
   content redirection 34
   data collectors 189
direct cable connections 204
ICA Administrator Toolbar 172
ICA audio settings 212
ICA browsing 81
ICA Client connections 195
ICA encryption 209
ICA network connections 125
IMA zones 189
MetaFrame XP administrators 78, 174
MetaFrame XP servers and farms 169–193
mixed mode operation 100
network firewalls 87
ODBC drivers 118
ports 92
printer autocreation in NDS 76
shadowing 123
user access to applications 248
Connection Control feature 266
connection licenses 141, 145
connections, controlling 266
content 251
publishing 243–244, 258, 260
enhancements to 34
publishing to be opened on client 259
publishing to be opened on server 258
content redirection 34, 243–244, 251
configuring 255
from client to server 251, 255
from server to client 256
controlling
access to the Management Console 175
client logons 265
conventions, documentation 15
counters, performance 288
CPU priority for applications 261
Ctxxmlss command 337

D

data collectors 189–190
election preference 191
response to UDP broadcasts 184
data store
see IMA data store 105
dial-in account properties 203
Dialin Information dialog box 203
direct cable connections 204
disconnecting ICA sessions 274
DNS address resolution 86
DNS and server names 45
documentation 14
conventions 15
ICA Clients 16
MetaFrame XP 14
online help, using 16
online Product Documentation Library 17
submitting comments 18
Web Interface for MetaFrame XP Administrator’s

Guide 14
documents and files, publishing 258
DOS-based printers 292
downgrading a feature release 130
drive mapping 214
Driveremap command 338
Drivers tab 297
Dscheck command 341
Dsmaint command 343

E
Edit Connection dialog box 202, 204
election of data collectors 191
encryption, configuring 209
explicit users 249
extended characters in server names 45
external IP addresses 316

F
feature release level 130, 155
feature releases 26
downgrading 130
features included in Feature Release 1 37
features included in Feature Release 2 33
features included in Feature Release 3 26
upgrading to 129
file type association 250
firewalls 55, 79, 81, 83, 87–90, 92

G
global groups 70
grace period for licenses 146

H
hardware requirements 45
HTML files 254

I
IBM DB2
creating an IMA data store 105
migrating to 65
requirements 64
using DB2 for the data store 117
ICA (Independent Computing Architecture) 22
ICA Browser 93–94
ICA browsing 80–82, 85, 87–91, 93
ICA Client Creator 227
ICA Client Distribution wizard 127, 229
ICA Client Object 224
ICA Client Update Database 224
ICA Clients
  automatic client update 227
  automatic reconnection 276
  client printers 291
  Client Update Configuration utility 229
  Client Update Database 229
  client update process 228
  Components CD 223
  connection licenses 145
  connections, limiting 267
  deploying 219–240
  deploying from network shares 226
  deploying with diskettes 227
  deploying with the Web Interface 238
  deployment methods 219–220
  deployment practices 236
  deployment scope 222
  downloading 17
  features 22
ICA Client Distribution wizard 127, 223, 229
ICA Client Object 224
ICA Client Update Database 224
installation diskettes, creating 227
installing using the Web Interface 222
logging activity 324
logons to servers, controlling 265–266
NDS logons 72
printer mapping 216
Program Neighborhood Agent 221
server location methods 83
server response to broadcasts 84, 184
shadowing 170
SSL support 38
time zone support 185
updating 227, 240
Web-based installation 238
with the Web Interface for MetaFrame XP 237
ICA connections 195–217
  adding 197
  asynchronous 46, 198, 204
  audio mapping 217
  client device mapping 214
  COM port mapping 217
  drive mapping 214
  Edit Connection dialog box 202
  encryption 209
  modem callback options 202
  network connections 125
  null modem cables 202
  printer mapping 216
  restricting connections 209
ICA Display options 183
ICA Encryption 160
ICA files 254
ICA session monitoring 39, 288
ICA sessions 81, 195, 241, 271
  browsing configuration 81
  configuring Auto Client Reconnect 276
  controlling logons 265
  disconnecting sessions 274
  encrypting 209
  monitoring session status 271
  performance monitoring 288
  published application data 271
  resetting sessions 275
  sending messages to users 274
  Session ID 273
  shadowing 170, 209, 284
  states of 273
  terminating processes 276
Icaport command 347
IMA 21–22, 92, 147, 184, 330
  changing the IMA port 348
  data collectors 189–190
  IMA service 77, 93, 141, 317
  zones 189
IMA data store 343
  configuring during Setup 116
  configuring ODBC drivers 118
  connecting to 54
  database choices 50
  migrating to IBM DB2 65
  migrating to Oracle 63
  migrating to SQL Server 60
  using IBM DB2 64, 105
  using Microsoft Access 55
  using MSDE 56
  using Oracle 61, 105
  using SQL Server 58, 105
  imaging MetaFrame XP servers 133
Imaport command 348
Independent Computing Architecture (ICA)
  see ICA
Independent Management Architecture (IMA)
  see IMA
installation
common Windows Installer commands 108
configuring ODBC drivers 118
configuring the IMA data store 116
creating a log file 109
creating an answer file for unattended installation 111
configuring Windows Installer transforms 110
feature release level, setting 130
imaging MetaFrame XP servers 133
MetaFrame Setup properties explained 367
MetaFrame XP 105, 117
product type 114
sample MetaFrame Setup transforms 368
shadowing restrictions 123
the Web Interface for MetaFrame XP 44
unattended installation 110
uninstalling MetaFrame XP 133–134
using Microsoft Access for the data store 116
using MSDE for the data store 56, 116
using SQL, Oracle, or IBM DB2 for the data store 117
using the MetaFrame XP Windows Installer package 108
Web Interface for MetaFrame XP 125
Internet Information Services 44
interoperability 93, 100
migrating MetaFrame 1.8 to MetaFrame XP 131
mixed mode 84
IP addressing 86, 91, 316
IP connectivity 83, 88
IP ports 24, 85, 92

J
Java objects 125
Java Run-Time Environment (JRE) 16, 47
Java Virtual Machine (JVM) 44
Jet database
   see Microsoft Access

L
licensing 137–157
activation 146
adding and activating multiple licenses 354
adding feature release licenses 155
assigning licenses 151
connection licenses 141
feature release licensing 154
grace period 139, 146
license counts 152–153
license numbers 146, 149
machine codes 146
MetaFrame for UNIX connection licenses 103
migrating from other products 141
overview of 137
pooling license counts 102, 153
product codes 139, 143
product licenses 140, 145
serial numbers 144
the Mlicense command 354
upgrading licenses 142
viewing license information 156
Load Manager 241
local printers 292
logons
   controlling 265
   reporting 324

M
machine codes 146
Management Console 173–182
controlling access to 175
selecting server farms 178
Management Console for MetaFrame XP 129
installing separately 134
Java Run-Time Environment 47
online help 16
updating 135
management tools 103, 169
master ICA Browser 93–94
messages, sending to users 274
MetaFrame 1.8 169
   interoperability 93, 100
   migrating to MetaFrame XP 131
MetaFrame for UNIX 103
MetaFrame XP
   overview of MetaFrame XP family of products 23
   setup options 113
   upgrading to feature releases 129
MetaFrame XP administrators 78
   creating customized administrators 175
deleagated administration of tasks 174
   delegating tasks 33
MetaFrame XP licensing
   see licensing
MetaFrame XP Server Administration 103
MetaFrame XP Universal Printing 306
Microsoft Access 55
Microsoft Internet Information Services 44
MigratetoMSDE command 350
migrating licenses 141
migrating MetaFrame 1.8 to MetaFrame XP 131
migrating to MetaFrame XP 131
mixed mode 84, 93, 100
server farm naming for 45
Mlicense command 351
modems 46
callback options 202
ICA connections with 202
monitoring ICA sessions 271, 288
moving a MetaFrame XP server to a different farm 330
MSDE
using for farm’s data store 56
msiexec command 108
N
names of servers and server farms 45
native mode 100
Active Directory 67, 70
MetaFrame XP 84–85, 101–104
NetWare drive mapping assignments 216
network connections 125
network firewalls 55, 79, 81, 83, 87–90, 92
network management, SNMP 186
network printers 292, 294, 299
network protocols 83, 88
New Connection dialog box 202
NFuse Classic
see Web Interface for MetaFrame XP
Novell Directory Service 72
Novell ZENworks 77
null modem cables, ICA connections with 202
O
ODBC drivers, configuring 118
online documentation 14
Oracle
creating an IMA data store 105
migrating to 63
requirements 61
using Oracle for the data store 117
P
parameter passing 253
parameters
passing to published applications 253
pass-through ICA Client 246
performance counters 288
performance monitoring 288
policies
about 34
configuring user-to-user shadowing with policies 286
creating a policy 282
prioritizing 283
ports used by MetaFrame XP software 92
print servers, importing 296
printer drivers 300
managing 297
printer management 291–306
client printer mapping 216
Drivers tab 297
importing print servers 296
installed printers 298
managing printer drivers 300
printer autocreation in NDS 76
replicating printer drivers 301
setting up network printers 299
user permissions 70
printers
bandwidth consumption 297
client 291, 293
local 292
managing 291
MetaFrame XP Universal Printing 306
network 292, 294, 299
printer drivers 300
shared 291
Printers tab 298
processes, terminating 276
product codes 139, 143
product licenses 145
product type 114
Program Neighborhood Agent 221
protocols, networking 83, 88
proxy servers 81
Published Application Manager 104
published content 251
publishing applications 244–255
CPU prioritization 261
data on running applications 271
license usage 153
limiting application instances 267
pass-through ICA Client 246
procedures 249
publishing content 258
standard applications 241
user authentication 245
user permissions 70
XML Service 125
publishing applications and content 244
publishing content 251, 258, 260

Q
Query command 356

R
reconnecting ICA Clients automatically 276
redirecting application launching 34
remote control
see shadowing ICA sessions
removing servers from server farms 133
replicating printer drivers 301
requirements
data store database 55
disk and memory 46
for running MetaFrame XP on Windows Server 2003 44
hardware 45
IBM DB2 64
Microsoft Access 55
MSDE 56
Oracle 61
SQL Server 58
system sizing 47
system software 43
Reset command 275
resetting ICA sessions 275

S
Secure Gateway for MetaFrame 159
securing MetaFrame deployments
with ICA Encryption 160
with the Secure Gateway 159
with Virtual Private Networks 160
securing MetaFrame XP deployments
with Citrix SSL Relay 159
security
ICA Encryption 160
Secure Sockets Layer (SSL) 162
Transport Layer Security (TLS) 162
sending messages to users 274
serial numbers 144
serial port mapping 217
server location 81–83, 85, 87–91, 93
server names, extended characters in 45
server-based computing 19
Session ID 273
sessions 195
see ICA sessions
setup
see installation
Shadow Taskbar 170, 285
shadowing 123, 170, 209, 284
user-to-user shadowing 34, 286
shared printers 291
sizing systems for MetaFrame XP 47
smart cards 34
software requirements 98
using SSConfigure 98
using with MetaFrame 97
SNMP network management 186
Solution Knowledgebase 17
SpeedScreen Browser Acceleration 28, 193
SQL Server
creating an IMA data store 105
migrating to 60
requirements 58
using SQL for the data store 117
SSConfigure 98
SSL
see Citrix SSL Relay
states of ICA sessions 273
system requirements
see requirements

T
TCP ports 92
SSL relay (443) 162
XML Service (80) 125
TCP/IP Network Protocol 84
TCP/IP+HTTP Network Protocol 83
terminating processes 276
time zone support 185
TLS 162
tools and utilities 103, 169, 171
transforms 368
Transport Layer Security (TLS) 162
Twconfig command 365

U
UDP broadcasts 83, 184
unattended installation 110
creating an answer file 111
creating Windows Installer transforms 110
uninstalling MetaFrame XP 133–134
universal groups 69
universal printer driver 306
updating ICA Clients 227, 240
upgrading MetaFrame 1.8 to MetaFrame XP 131
user account properties 203
user groups 248
user permissions 70
user policies 34
 creating a policy 282
 prioritizing 283
User Properties dialog box 203
user-to-user shadowing 286
using MetaFrame XP with MOM/WMI 31
utilities 311–366

V
virtual printers 291
Virtual Private Networks 160

W
Web Interface
 XML Service 125
Web Interface for MetaFrame XP 14, 44, 79, 85–86, 90, 125, 221, 237–238
setting the MetaFrame XP server’s default Web page 127
Web-based ICA Client installation 238
WinCE 292
Windows Installer
 common commands 108
 creating a log file when installing MetaFrame 109
 creating transforms 110, 367
 installing MetaFrame XP using the Windows Installer package 108
 msiexec command 108, 113
Windows Installer transforms 367
 sample MetaFrame Setup transforms 368

X
XML
 Citrix XML Service 85, 125
data 83
XML Service 125, 337

Z
ZENworks Dynamic Local Users 77
 zones 189
 see IMA zones